FINANZWISSENSCHAFTLICHE SCHRIFTEN

Knut Blind

Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten

Fallstudie: Informationssicherheit in Kommunikationssystemen



FINANZWISSENSCHAFTLICHE SCHRIFTEN

Knut Blind

Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten

Das Informations- und Kommunikationszeitalter löst neue Risiken für die Datensicherheit von Kommunikationsverbindungen und damit entsprechenden staatlichen Handlungsbedarf aus. Ausgehend von der Erwartungsnutzentheorie wird zunächst das optimale Ausmaß an Sicherheitsmaßnahmen abgeleitet. Sodann werden Ursachen für Fehlallokationen identifiziert und wirtschaftspolitische Lösungsmöglichkeiten dargestellt. Eine Fallstudie thematisiert die potentielle Gefährdung der Informationssicherheit in offenen Kommunikationsnetzen. Es folgt eine Analyse der privatwirtschaftlichen Versicherbarkeit dieser Risiken. Nachfolgend werden Gründe aufgezeigt, warum sich in einem deregulierten Telekommunikationsmarkt keine effiziente Informationssicherheit einstellen kann. Das Schlußkapitel unterbreitet konkrete Vorschläge, wie den drohenden Gefahren in der Bundesrepublik Deutschland zu begegnen ist.

Knut Blind wurde 1965 in Schwäbisch Hall geboren. Sein Studium der Volkswirtschaftslehre in Freiburg und St. Catherines/Kanada schloß er 1992 in Freiburg mit dem Diplom ab. Seit 1993 ist er Assistent am Institut für Finanzwissenschaft der Universität Freiburg. Außerdem wirkt er am 1994 ins Leben gerufenen interdisziplinären Forschungsprojekt "Sicherheit in der Kommunikationstechnik" der Gottlieb Daimler- und Carl Benz-Stiftung mit 1995 hat er bei Prof. Dr. Hans-Hermann Francke promoviert.

Retrodigitization in 2018

www.peterlang.com

Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten
Fallstudie: Informationssicherheit in Kommunikationssystemen

FINANZWISSENSCHAFTLICHE SCHRIFTEN

Herausgegeben von den Professoren
Albers, Krause-Junk, Littmann, Oberhauser, Pohmer, Schmidt

Band 74



Knut Blind

Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten

Fallstudie:
Informationssicherheit in Kommunikationssystemen



PETER LANG
Europäischer Verlag der Wissenschaften

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Blind, Knut:

Allokationsineffizienzen auf Sicherheitsmärkten : Ursachen und Lösungsmöglichkeiten ; Fallstudie: Informationssicherheit in Kommunikationssystemen / Knut Blind. - Frankfurt am Main ; Berlin ; Bern ; New York ; Paris ; Wien : Lang, 1996
(Finanzwissenschaftliche Schriften ; Bd. 74)
Zugl.: Freiburg (Breisgau), Univ., Diss., 1995
ISBN 3-631-49524-2

NE: GT



This book is available Open Access thanks to the kind support of ZBW – Leibniz-Informationszentrum Wirtschaft.

D 25
ISSN 0170-8252
ISBN 3-631-49524-2
ISBN 978-3-631-75166-4 (eBook)

Printed in Germany 1 2 4 5 6 7

Vorwort

Die vorliegende Dissertation ist das Ergebnis meiner Untersuchungen im Rahmen des interdisziplinären Forschungsprojekts „Sicherheit in der Kommunikationstechnik" der Gottlieb Daimler- und Carl Benz-Stiftung. Dieser bin ich doppelt zu Dank verpflichtet: Zum einen wurde mein Vorhaben durch ihre finanzielle Unterstützung in Form von Drittmittelgeldern erst ermöglicht. Zum anderen habe ich im Rahmen der von ihr veranstalteten Kollegsitzungen durch den inhaltlichen Austausch mit den Vertretern anderer wissenschaftlicher Disziplinen Anregungen für meine ökonomische Analyse erhalten.

Ein weiterer Baustein im Entstehungsprozeß meiner Dissertation war meine Tätigkeit am Institut für Finanzwissenschaft der Universität Freiburg, in welchem stets eine kreative und kollegiale Arbeitsatmosphäre herrschte. Deshalb möchte ich allen Kollegen meinen Dank aussprechen, die in unterschiedlichster Weise ihren Beitrag zum Gelingen der vorliegenden Arbeit geleistet haben. Namentlich möchte ich hier besonders Diplom-Volkswirtin Judith Safford herausheben, mit der ich Büro und zeitweilig den PC geteilt habe.

Schließlich gilt mein besonderer Dank dem Erstgutachter der Arbeit und meinem Doktorvater Herrn Professor Dr. Hans-Hermann Francke, dessen persönliches Engagement meiner Mitarbeit am angesprochenen Forschungsprojekt vorausging und der mir die erfolgreiche Bearbeitung dieses für einen Ökonomen ungewöhnlichen Terrains auch zugetraut hat. Ferner habe ich Herrn Professor Dr. Günter Müller, dem Zweitgutachter und Leiter des Kollegs „Sicherheit in der Kommunikationstechnik", zu danken. Für die Aufnahme meiner Arbeit in die Reihe „Finanzwissenschaftliche Schriften" ist Herr Professor Dr. Alois Oberhauser verantwortlich, dem ich hierfür meinen Dank aussprechen möchte.

Zu guter letzt danke ich all meinen Freunden und vor allem meiner Freundin Ulrike Gude für die gemeinsamen Zeiten während meiner Promotion, in denen die Ökonomie nicht im Mittelpunkt stand.

Freiburg im August 1995 Knut Blind

Inhaltsverzeichnis

Abbildungsverzeichnis

Übersichtsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
AG	Aktiengesellschaft
ATM	Asynchroner Transfer Mode
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BK	Breitband-Kommunikation,
BMPT	Bundesministeriums für Post und Telekommunikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzgl.	bezüglich
bzw.	beziehungsweise
CCITT	International Telegraph and Telephone Consultive Committee
c. p.	ceteris paribus
DBP	Deutsche Bundespost
DM	Deutsche Mark
d. h.	das heißt
EG	Europäische Gemeinschaft
ETSI	European Telecommunication Standard Institute
GSM	Global System for Mobile Communication
IDN	Integriertes Text- und Datennetz
IN	Intelligentes Netz
ISDN	Integrated Service Digital Network
ISO	International Standard Organization
ITSEC	Information Technology Security Evaluation Criteria
ITU-S	International Telecommunication Union - Standardization
i. e. S.	im engeren Sinn
i. d. R.	in der Regel
KES	Zeitschrift für Kommunikations- und EDV-Sicherheit
Mrd.	Milliarden
OSI	Open System Interconnection
ProdHaftG	Produkthaftungsgesetzes
PTRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
SAGE	Security Algorithms Group of Experts

SOGIS	Senior Officials Group for Information Security
STAG	Security Technology Advisory Group
TDSV	Telekom-Datenschutzverordnung
TKV	Telekommunikationsverordnung
UDSV	Teledienstunternehmen-Datenschutzverordnung
UmweltHG	Umwelthaftungsgesetz
u.	und
u. a.	unter anderem / und andere
u. U.	unter Umständen
VBN	Vorläufer-Breitband-Netz
v. a.	vor allem
vgl.	vergleiche
WIK	Wissenschaftliches Institut für Kommunikationsdienste
wg.	wegen

Symbolverzeichnis

a	Handlungsalternativen
AC(.)	Durchschnittskostenfunktion
AR(.)	absolute Risikoaversion
ASI(.)	asymmetrische Informationsverteilung
c	Aufwand an Self-insurance
C(.)	Kostenfunktion
d	Deckungsgrad
Δ	Differenz
∂	partielle Ableitung
E	Ergebnismatrix
E(.)	Erwartungswert
ES	Erwartungsschaden
EXT(.)	Externalitäten
f(.)	variable Kostenfunktion
F(.)	Fixkostenfunktion
I	Integrationsgrad
IM(.)	immaterielle Nutzenkomponente
K	Kompensation
l	Anzahl der Schadensarten
L	Schadenhöhe
ma	mark-up bzw. Aufschlag
MB	Grenznutzen
n	Teilnehmerzahl
p	Eintritts- bzw. Schadenswahrscheinlichkeiten
P	Versicherungsprämie/Preis
q	Schadenswahrscheinlichkeit plus Aufschlag ma
r	Aufwand an Self-protection
R	Risikoprämie
s	Aufwand an kombinierten Schutzmaßnahmen
S	zukünftige Naturzustände
SÄ	Sicherheitsäquivalent
TC(.)	Gesamtkostenfunktion
U(.)	Nutzenfunktion
w_{as}	Konsequenz bzw. Vermögen in der zukünftigen Situation s bei Wahl der Handlungsalternative a
W	Ausgangsvermögen

1. Teil: Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten

1.1 Einleitung

1.1.1 Zur allgemeinen Thematik und Problemstellung

Mit der zunehmend komplexer werdenden Gesellschaft haben sowohl die durch technische Defekte ausgelösten als auch die durch kriminelle Aktivitäten hervorgerufenen Gefahren für die einzelnen Individuen in Umfang und Vielfalt zugenommen. Schon lange in der allgemeinen und in der ökonomischen Diskussion sind die Bedrohungen, mit denen die Menschen im Arbeitsleben und im Straßenverkehr konfrontiert werden. Durch den Übergang von der Industrie- zur Informations- und Kommunikationsgesellschaft entstehen neue Risiken und Gefahren, die zum einen wegen der starken Abhängigkeit der Konsum- und Produktionsphäre von diesen Hochtechnologien verursacht werden und die zum anderen auch neue Formen illegaler Aktivitäten wie der Computerkriminalität ermöglichen.

Die Individuen reagieren aktiv auf die Bedrohungspotentiale, die neben ihrer materiellen Position auch ihre Gesundheit oder sogar ihr Leben beeinträchtigen können. Aus diesem Grund schließen sie Versicherungen ab und ergreifen Sicherheitsmaßnahmen. Die volkswirtschaftlich schon immer bedeutenden Versicherungsmärkte sind in zahlreichen ökonomischen Untersuchungen auf ihre Allokationseffizienz hin geprüft worden. Dabei stellte sich heraus, daß Fehlallokationen vor allem durch das Informationsdefizit der Anbieter bezüglich des Risikopotentials der Versicherten ausgelöst werden.[1] Die Märkte für Sicherheitstechnologien und -systeme, die von einfachen Vorhängeschlössern über Alarmanlagen bis hin zu Überwachungssystemen industrieller Fertigungsanlagen reichen, sind in der Bundesrepublik Deutschland Sektoren, die z. T. jährliche Wachstumsraten von über 10% aufweisen. So wird für 1994 ein Umsatz von rund 14,5 Mrd. DM erwartet.[2] Dabei stellt sich auch für diese Märkte im ersten Teil der Arbeit die Frage nach effizienter Allokation und nach Ursachen für Suboptimalitäten. Obwohl sich eine Reihe von Ökonomen vor allem speziellen Fragestellungen, wie denen des Ver-

---

1 Vgl. Strassl (1988).
2 Vgl. o. V. (1994a), S. 29.

braucherschutzes[3] oder der Verkehrssicherheit[4], angenommen hat, fehlt eine rein theoretische Untersuchung, die - ausgehend von der Bestimmung eines Allokationsoptimums - Ursachen von Fehlallokationen identifiziert.[5] Letztere sind aber durchaus existent. Denn mit der hohen Komplexität der Produktionstechnik und der Konsumgüter ist unmittelbar das Problem verbunden, daß die von den Risiken Betroffenen nur eine unzureichende Kenntnis über das sie bedrohende Schadenpotential haben. Des weiteren fügen Unfälle im Produktionsprozeß und bei Konsumaktivitäten nicht nur dem direkt involvierten Opfer, sondern auch indirekt beteiligten Individuen Schaden zu. Schließlich haben die Wirtschaftssubjekte grundsätzlich das Problem, daß sie in Entscheidungssituationen unter Unsicherheit zu ökonomisch irrationalem Verhalten neigen. Aus diesen Gründen leitet sich unmittelbar staatlicher Handlungsbedarf ab. Das Spektrum reicht von marktkonformen rechtlichen Regelungen über staatliche Regulierungsmaßnahmen bis hin zum direkten staatlichen Eingriff in Form der staatlich gewährten öffentlichen Sicherheit. Hier hat aber inzwischen auch in der Bundesrepublik Deutschland eine teilweise Privatisierung eingesetzt.[6]

Mit dem anbrechenden Informations- und Kommunikationszeitalter haben sich auch die Bedrohungspotentiale verändert. Im Anschluß an informationstechnische Arbeiten[7] folgten bereits gesellschaftswissenschaftliche[8] und juristische[9] Abhandlungen über die Gefahren und mögliche Gegenmaßnahmen in einer Gesellschaft, die zukünftig verstärkt von Kommunikationssystemen abhängig sein wird. Bisher aber haben ökonomische Analysen über die Informations- und Kommunikationsbranche diese Sicherheitsaspekte vernachlässigt.

Der zweite Teil dieser Arbeit versucht deshalb, im Rahmen einer Fallstudie zunächst ökonomische Effizienzbedingungen für Sicherheitsvorkehrungen in Kommunikationssystemen herauszuarbeiten. Danach wird untersucht, warum die Marktkräfte[10] allein auf den zukünftigen Datenautobahnen kein volkswirtschaftlich

---

[3] Vgl. u. a. Asch (1988).

[4] Vgl. u. a. Moses & Savage (1989).

[5] Die Arbeit von Jones-Lee (1989) wird diesem Anspruch vielleicht noch am ehesten gerecht.

[6] Vgl. zur Kommerzialisierung öffentlicher Sicherheit durch private Wach- und Sicherheitsunternehmen, deren Umsatz inzwischen 4 Mrd. DM überschritten hat, Petersen (1994), (1994a).

[7] Vgl. u. a. Pfitzmann (1990).

[8] Vgl. Roßnagel, Wedde, Hammer und Pordesch (1989).

[9] Vgl. Wildhaber (1993).

[10] Vgl. zum Gestaltungsbedarf der neuen Informations- und Kommunikationssysteme aus soziologischer Perspektive Groebel (1994), S. 78.

optimales Sicherheitsniveau realisieren werden.[11] Schließlich werden nach ökonomischen Effizienzkriterien abgeleitete Empfehlungen ausgesprochen, die sich auf mögliche staatliche Eingriffe in die Informationssicherheit der zukünftig liberalisierten Telekommunikationsmärkte beziehen.

1.1.2 Zum Vorgehen und zur Methodik

Der erste, allgemeine Teil der Arbeit konzentriert sich auf die theoretische Bestimmung des Allokationsoptimums auf sogenannten Sicherheitsmärkten. Hier handelt es sich um Märkte, auf denen Sicherheitssysteme wie Alarmanlagen von Sicherheitstechnikherstellern oder Dienstleistungen von Wachgesellschaften angeboten und von Privatpersonen und Unternehmen nachgefragt werden. Dabei wird methodisch auf die vor allem in der Versicherungsökonomik angewandte Erwartungsnutzentheorie zurückgegriffen. Ferner wird die First-Best-Lösung des Versicherungsmarktes, sowohl Substitut als auch Komplement zu den Sicherheitsmärkten, dargestellt. Im folgenden Schritt wird unter Anwendung industrieökonomischer Erkenntnisse zuerst die Angebotsseite und anschließend mit Hilfe des mikroökonomischen Instrumentariums die Nachfrageseite auf mögliche Ursachen für Allokationsineffizienzen auf Sicherheitsmärkten untersucht.[12] Hier wird deutlich, daß es drei mögliche Ursachen für Allokationsineffizienzen im Bereich der Sicherheitsgüter gibt. Zu berücksichtigen sind vor allem das irrationale Nachfragerverhalten, die Informationsdefizite, die auch daraus resultierenden Informationsasymmetrien und die externen Effekte. Das letzte Kapitel des ersten allgemeinen Teils der Arbeit widmet sich verschiedenen staatlichen Instrumenten der Wirtschaftspolitik, die zur Behebung oben genannter Ursachen von Wohlfahrtsverlusten beitragen können. Es werden Möglichkeiten der Informationspolitik, des Haftungsrechtes, der direkten finanziellen Beeinflussung mittels Besteuerung und Subventionierung, der staatlichen Regulierung durch Mindestsicherheitsstandards und der unmittelbaren staatlichen Bereitstellung von Sicherheitsgütern dargestellt. Jeweils daran anschließend folgt eine Bewertung der verschiedenen Instrumente nach mikroökonomischer Allokationseffizienz, nach Verteilungsgerechtigkeit im Sinne des Verursacherprinzips und nach den anfallenden administrativen und fiskalischen Kosten.

---

[11] Vgl. zur Sicherheit auf Datenautobahnen Fuhrberg (1995).

[12] Der Begriff Marktversagen, vgl. dazu Fritsch, Wein und Ewers (1993), ist eigentlich nicht angebracht, weil es nicht zu einem gänzlichen Zusammenbruch des Marktes für Sicherheitsgüter kommt. Deshalb wird vornehmlich der Begriff Allokationsineffizienz verwandt.

Im zweiten Teil der Arbeit wird das im ersten Teil entwickelte allgemeine Verfahren in Form einer Fallstudie auf die spezielle Problematik der Informationssicherheit in öffentlich zugänglichen Kommunikationssystemen angewandt. Diese Art Sicherheit beinhaltet einen umfassenden Schutz der Kommunikationsbeziehungen vor beabsichtigten oder zufälligen Beeinträchtigungen. Nach einem Überblick über das aktuelle Angebot an Kommunikationsnetzen und -diensten wird eine Charakterisierung nach ökonomischen Kriterien vorgenommen, wo Kommunikationssysteme im Spektrum zwischen reinen privaten und öffentlichen Gütern den Clubgütern zugerechnet werden. Auf die Clubgüter-Theorie von Buchanan (1965) aufbauend werden die Nutzenmaximierungskalküle der Teilnehmer hinsichtlich gewünschter Größe und Leistungsfähigkeit von Kommunikationssystemen dargestellt. Nach einer Analyse der ökonomischen Implikationen von Informationssicherheit in Kommunikationssystemen und einer sicherheitsökonomischen Charakterisierung von Informationssicherheitsmaßnahmen werden Kosten- und Nutzenfunktion der Informationssicherheitsmaßnahmen in Abhängigkeit der Netzeigenschaften formalisiert. Damit läßt sich eine qualitative Aussage über die Beziehung zwischen den Eigenschaften der Kommunikationssysteme und dem optimalen Niveau an Informationssicherheit treffen.[13]

In einem eigenen Kapitel werden die Versicherungsmöglichkeiten von Risiken aus Verletzungen der Informationssicherheit unter Berücksichtigung des aktuellen Versicherungsangebotes in der Bundesrepublik Deutschland untersucht und mögliche staatliche Eingriffe diskutiert. Daran anschließend wird der Frage nachgegangen, ob es hinsichtlich der Informationssicherheit in Kommunikationssystemen zu Allokationsineffizienzen kommen kann. Als Ursachen werden Informationsdefizite und -asymmetrien und negative Externalitäten identifiziert. Im Schlußkapitel werden Vorschläge ausgearbeitet, wie mit Hilfe des bereits vorgestellten Instrumentariums unter Berücksichtigung der institutionellen Gegebenheiten in der Bundesrepublik Deutschland die Informationssicherheit in offenen Kommunikationsnetzen verbessert werden kann. Ziel ist es, drohende volkswirtschaftliche Wohlfahrtsverluste zu begrenzen.

Die Anwendung neoklassischer Wohlfahrts- und Allokationstheorie auf die Thematik „Informationssicherheit in Kommunikationssystemen“ ist mit einer Reihe von Problemen behaftet und bietet somit folgende Angriffsflächen. Zum einen wird

---

[13] Ein Vergleich mit dem aktuellen Stand der Implementierung von Informationssicherheitsmechanismen erübrigt sich, weil im Moment lediglich die Funkstrecken der Mobilfunknetze verschlüsselt sind.

man mit großen Schwierigkeiten hinsichtlich der qualitativen und quantitativen Bestimmung von Bedrohungspotentialen konfrontiert, mit der die Praxis ebenfalls zu kämpfen hat.[14] Zum anderen ist man durch das ökonomisch theoretische Vorgehen zu einer Abstraktion von technischen Gegebenheiten gezwungen, wodurch die gezogenen Schlüsse in Frage gestellt werden können. Dieser Gefahr ist jedoch zum Beispiel auch die Industrieökonomie generell ausgesetzt, wenn sie sich mit der Ökonomie von Kompatibilitätsstandards in der Telekommunikation auseinandersetzt. Des weiteren handelt es sich bei der Informationssicherheit um ein Feld, dessen Teilbereich „Datenschutz“ starken rechtlichen Regelungen unterworfen ist. Diese reichen sogar bis hin zum Grundrechtsschutz. Grundrechtliche Fragestellungen sollten aber für ökonomische Analysen aufgrund ethischer Wertvorstellungen tabu sein. Aber selbst in der Rechtspraxis und -theorie gibt es eine Abwägung zwischen Rechtsgütern, wie der aktuelle rechtliche Konflikt zwischen dem Grundrecht auf informationelle Selbstbestimmung in Form des Fernmeldegeheimnisses und der Gewährleistung innerer Sicherheit mit den daraus folgenden Kostenbelastungen zeigt.[15] Die ökonomische Analyse des Rechts unerlaubter Handlung und der Produkthaftung kann aber dazu beitragen, die Opportunitätskosten unterschiedlicher rechtlicher Regelungen aufzuzeigen. Trotzdem wurde auf eine ökonomische Analyse der Wirkungen des Strafrechts auf das Ausmaß kriminell motivierter Verletzungen der Informationssicherheit verzichtet und der strafrechtliche Rahmen als gegeben angenommen.[16] Denn der Abschreckungseffekt einer strafrechtlichen Verfolgung muß als begrenzt angesehen werden, da sich die Identifikation der Täter schwierig gestaltet. Ferner verändert die Verschärfung des Strafrechts lediglich einen exogenen Parameter ohne die abgeleiteten Ergebnisse qualitativ zu beeinträchtigen. Schließlich verhindert die hohe Dunkelziffer im Bereich der Computerkriminalität eine empirische Überprüfung der theoretisch abgeleiteten Ergebnisse. Dies gilt jedoch für diese Thematik generell. Im Gegensatz zu Arbeiten über Arbeitsplatzrisiken oder Straßen- und Luftverkehrssicherheit existieren hinsichtlich der Sicherheit von Kommunikationsnetzen keine Datenmaterialien, die eine empirische Überprüfung der theoretisch gewonnenen Ergebnisse erlauben. Auch in Zukunft wird damit nicht zu rechnen sein, weil eine exakte Dokumentation dieser Schadensfälle folgenden Schwierigkeiten ausgesetzt ist. Zum einen behindern hohe

---

[14] Vgl. dazu u. a. Moser (1995).

[15] Vgl. zur Kontroverse über die Abhörbarkeit der D-Netze o. V. (1995d), (1995e).

[16] Nach der KES-Sicherheitsstudie von Gartner & Konrad (1994), S. 2, ist der Anteil kriminell motivierter Schadensfälle im Gegensatz zur allgemeinen Einschätzung relativ gering.

Dunkelziffern eine genaue Erfassung. Gleichzeitig können die identifizierten Schadensfälle nur bedingt in Geldeinheiten gemessen werden.

Obwohl quantitative Ergebnisse mit Hilfe eines solchen Vorgehens nicht abgeleitet werden können, versucht die folgende ökonomische Analyse der Informationssicherheit in offenen Kommunikationssystemen dennoch, qualitative Erkenntnisse zu gewinnen.

1.2 Die nutzenmaximierende Allokation verschiedener Sicherheitsstrategien

1.2.1 Vorbemerkungen

Ziel des ersten Kapitels ist es, in einem mikroökonomischen Modellrahmen die individuellen Optima hinsichtlich verschiedener Sicherheitsgüter und -vorkehrungen abzuleiten. Neben der Angebotsseite, auf deren Besonderheiten im nächsten Kapitel eingegangen und die deshalb zunächst als einfache Grenzkostenfunktion modelliert wird, werden vor allem die Nachfragedeterminanten differenzierter analysiert, weil sie die Grundlage für die Analyse von Ineffizienzen auf dem Markt für Schadensgüter bzw. Schadenspräventionsmaßnahmen bilden werden.

Vor der eigentlichen theoretischen Analyse müssen einige Vorbemerkungen zum Vorgehen gemacht werden. Es bestehen grundsätzlich zwei Möglichkeiten, die Sicherheit von Konsum- oder Produktionsgütern bzw. -aktivitäten mikroökonomisch zu analysieren. Die herkömmliche Vorgehensweise faßt die Produktsicherheit als eine von mehreren Eigenschaften des betrachteten Gutes auf und analysiert die entsprechenden Märkte vor dem Hintergrund differenzierter Qualitäten bzw. Sicherheitseigenschaften.[17] Die Sicherheitsqualitäten des Produktes werden also als Verschiebungsparameter der Angebots- und Nachfragefunktionen in ein mikroökonomisches Marktdiagramm integriert.[18] Es wird hier ein anderer Analyseansatz gewählt, welcher auf folgender Ausgangssituation basiert.[19] Das betrachtete Individuum besitzt bereits ein Produktions- oder Konsumgut, bei dessen Benutzung mit einer bestimmten Wahrscheinlichkeit Schäden auftreten können. Das Entscheidungsproblem für das Individuum besteht nun darin, vor seiner Nutzung das optimale Ausmaß an Sicherheitsvorkehrungen zu treffen. Diese Vorgehensweise wurde gewählt, um die Interdependenzen zwischen der Nachfrage nach Sicherheitsgütern und dem Marktgleichgewicht für risikobehaftete Güter auszuklammern, weil da-

---

[17] Diese Darstellungsart wird der Realität auch in den meisten Fällen gerecht, weil Sicherheitsausstattungen i. d. R. bereits in den meisten Produkten, welche im folgenden als Basisgüter oder -produkte bezeichnet werden, integriert und separat überhaupt nicht zu erwerben sind.

[18] Vgl. dazu u. a. Oi (1973) und Adams (1987).

[19] Vgl. dazu Hiebert (1983), der solch eine Analyse für die Situation eines Unternehmens durchführt. Der zusätzliche Erkenntnisgewinn ist für diese Arbeit eher unwesentlich, so daß die theoretische Analyse vom Aktivitätsniveau abstrahiert. Jedoch kann dieses auch in Form eines exogenen Parameters in den Nachfragefunktionen Berücksichtigung finden. Eine neuere Studie von Cicchetti & Dubin (1994), S. 169-186, bekräftigt diese Vorgehensweise, weil sie die Erwartungsnutzentheorie an dem praktischen Beispiel der Nachfrage nach einer Versicherung gegen Telefonleitungsstörungen testet.

durch das Aktivitätsniveau, d. h. die individuelle Nutzungsintensität des Produktes, als weiterer Entscheidungsparameter zu berücksichtigen ist.[20] Diese Verfahrensweise wird auch vor dem Hintergrund der Fallstudie gewählt, weil es sich bei einem Anschluß an ein Kommunikationsnetz um eine Entweder-Oder-Entscheidung handelt und die Nutzungsintensität von zweitrangiger Bedeutung ist.

Das Kapitel ist wie folgt aufgebaut. Zunächst werden allgemein Entscheidungen unter Unsicherheit genauer charakterisiert, bevor die individuellen Optima an verschiedenen Präventionsmöglichkeiten, einschließlich Versicherung, theoretisch abgeleitet werden.

1.2.2 Zur Entscheidungsfindung unter Unsicherheit

Jedes Wirtschaftssubjekt muß permanent ökonomisch relevante Entscheidungen treffen.[21] Die ökonomische Theorie hat schon frühzeitig begonnen neben den Situationen, in welchen alle entscheidungsrelevanten Parameter ex ante bekannt sind, die Entscheidungsfindung unter Unsicherheit zu untersuchen.[22] Bei Unsicherheit entscheidet das Schicksal bzw. die Natur über die Ausprägung einer Teilmenge der für die Entscheidung relevanten Variablen. Das Individuum muß sich aber ex ante ohne Wissen über die zukünftige Konstellation für eine Handlungsalternative entscheiden.

1.2.2.1 Prämissen

Für die Analyse eines Entscheidungsproblems dieser komplexen Art müssen eine Reihe von vereinfachenden Annahmen gemacht werden, um überhaupt Erkenntnisse gewinnen zu können. Deshalb berücksichtigt das Individuum bei seiner Entscheidungsfindung unter Unsicherheit explizit nur folgende Faktoren:

---

[20] Einen ähnlichen Ansatz wählen Epple & Raviv (1978), S. 81f.

[21] Vgl. zu den allgemeinen Grundlagen der Entscheidungsfindung Sinn (1980), S. 5-8, und Varian (1992), S. 94-97.

[22] Vgl. dazu die Darstellungen in Hirshleifer & Riley (1992), S. 7-42, und Sinn (1980), S. 5-46, wobei letzterer einen umfassenden Literaturüberblick bietet.

(1) Das Wirtschaftssubjekt kennt alle entscheidungsrelevanten zukünftigen Naturzustände S.[23]

(2) Diesen Zuständen kann es die jeweiligen Eintrittswahrscheinlichkeiten p_s zuordnen.

(3) Seinen möglichen Handlungsalternativen a kann der Entscheidende für jedes potentielle Zukunftsszenario die entsprechenden Konsequenzen w_{aS} zuordnen, wobei diese aus Gründen der Operationalisierbarkeit in monetären Werten gemessen werden.[24]

(4) Das Individuum besitzt eine stetig steigende Nutzenfunktion $U(w_{aS})$, welche es ihm ermöglicht, jedem monetären Wert einen Nutzenwert zuzuordnen.

(5) Das Wirtschaftssubjekt hat eine Bewertungsfunktion - nach Sinn Präferenzfunktional - , welche es ihm erlaubt, "aus der Menge der verfügbaren Handlungsalternativen eine solche [auszuwählen], die zu einer Wahrscheinlichkeit des Periodenendvermögens führt, deren Präferenzfunktional von keiner anderen Verteilung übertroffen wird"[25].

Schließlich wird dem Individuum unterstellt, daß es im Vollbesitz seiner geistigen Kräfte ist, d. h. das Individuum ergreift die gemäß seinem Präferenzfunktional beste Handlungsalternative bei gegebenem Wissen über die Menge der möglichen Zustände und der ihnen jeweils zugeordneten Wahrscheinlichkeiten.[26]

---

23 Hier wird der Begriff Unsicherheit verwendet, der sich auf einen geschlossenen Wahrscheinlichkeitsraum mit bekannten Ereignissen und Wahrscheinlichkeiten bezieht. Der übergeordnete Begriff Ungewißheit geht von einem offenen Wahrscheinlichkeitsraum aus, was zwar eher realistischen Entscheidungssituationen entspricht, jedoch in der theoretischen Analyse nicht operationalisierbar ist, weil damit nicht mehr alle zukünftigen Zustände S bekannt sind.

24 Die Begrenztheit dieser Vorgehensweise wird besonders beim Verlust nicht-reproduzierbarer Vermögens- und sonstiger Werte deutlich. Es wird bzgl. dieser Problematik in Teil 1 von einer Annahme der ökonomischen Analyse des Rechtes Gebrauch macht, welche davon ausgeht, daß für alle entstehenden Schäden Geldäquivalente existieren. Vgl. dazu Endres (1991), S. 15.

25 Sinn, (1980), S. 48.

26 Die Handlungsalternativen - "terminal moves" - des Individuums können erweitert werden, indem "informational actions", welche das Wissen über die gegebene Situation verbessern, zugelassen werden. Hierunter fallen weitere Nachforschungen über Schadeneintrittswahrscheinlichkeiten. Jedoch wird der Ökonomie von Informationssuchprozessen hier nicht weiter nachgegangen. Vgl. zu dieser Unterscheidung Hirshleifer & Riley (1992), S. 8f. Die damit verbundene Problematik der Informationsasymmetrien wird in Abschnitt 1.4.3 näher untersucht.

1.2.2.2 Zur Problematik der Wahrscheinlichkeiten

In den oben genannten Annahmen über die Entscheidungsfindung bei Unsicherheit wurde als selbstverständlich postuliert, daß die Individuen fähig sind, den zukünftigen Zuständen Wahrscheinlichkeiten zuzuordnen. Jedoch bedarf diese Prämisse einer näheren Erläuterung, welche sich mit dem Wahrscheinlichkeitsbegriff genauer auseinandersetzt. Allgemein ist Wahrscheinlichkeit definiert als ein Maß zur Quantifizierung der Sicherheit bzw. Unsicherheit des Eintretens eines Ereignisses im Rahmen eines Zufallsexperiments.[27]

Da die strikten Annahmen des klassischen Wahrscheinlichkeitsbegriffs nur auf einfache Zufallsexperimente, wie auf das Münzwurfbeispiel, anwendbar sind, muß man sich bei komplexen realen Problemstellungen auf den statistischen und subjektiven Wahrscheinlichkeitsbegriff beschränken. Die Wahrscheinlichkeit für das Eintreten eines Ereignisses ist nach dem statistischen Wahrscheinlichkeitsbegriff der Grenzwert der relativen Häufigkeit des Auftretens des entsprechenden Ereignisses bei einer Folge identischer und unabhängiger Versuche. Falls die Anzahl der Versuche hinreichend groß ist, dann entspricht dieser Wahrscheinlichkeitsbegriff dem, was im allgemeinen unter objektiver Wahrscheinlichkeit verstanden wird.

Nachdem es in vielen Entscheidungssituationen nicht möglich ist, objektive Wahrscheinlichkeiten nach dem statistischen Wahrscheinlichkeitsbegriff zu bestimmen, weil es sich um neuartige oder gar einzigartige Konstellationen handelt, muß man sich eigentlich auf den subjektiven Wahrscheinlichkeitsbegriff beschränken.[28] Savage (1954) als Hauptvertreter der subjektivistischen Sichtweise war der Überzeugung, daß als Entscheidungsgrundlage aller individuellen Entscheidungen nur subjektive Wahrscheinlichkeiten dienen. So unterstellt er den Individuen, daß diese selbst bei einem kontrollierten Zufallsexperiment von der Art eines Urnenbeispiels nicht auf die objektiven Wahrscheinlichkeiten zurückgreifen.[29]

Es ist zwar einleuchtend, daß die Wirtschaftssubjekte ihren Entscheidungen unter Unsicherheit subjektive Wahrscheinlichkeiten zugrunde legen, jedoch resultiert

---

27 Vgl. Bleymüller, Gehlert und Gülicher (1991) S. 27, und ebenda S.27f, bzgl. der verschiedenen Wahrscheinlichkeitsbegriffe.

28 Der Hauptgrund für die Nichtanwendbarkeit des statistischen Wahrscheinlichkeitsbegriffes liegt darin, daß für die Bestimmung einer relativen Häufigkeit eine hinreichend große Zahl von identischen Experimenten abgelaufen sein muß und dies i. d. R. nur bei realitätsfernen Laborexperimenten möglich ist.

29 Vgl. Savage (1954), S. 63-67.

daraus das methodische Problem, daß keine objektiv überprüfbaren Wahrscheinlichkeiten mehr existieren und damit kein Referenzrahmen für die normative Bewertung von Entscheidungen unter Unsicherheit zur Verfügung steht. Um der Theorie der Entscheidung unter Unsicherheit Aussagekraft verleihen zu können, müssen jedoch objektive Wahrscheinlichkeiten gegeben sein. Diese lassen sich aus den subjektiven Wahrscheinlichkeiten ableiten, indem das Individuum abzuschätzen versucht, mit welcher relativen Häufigkeit die verschiedenen Zustände bei vielfachen fiktiven Wiederholungen der Entscheidungssituation auftreten werden.[30]

Diese Vorgehensweise zeichnet sich durch eine Reihe von Vorteilen aus. Zum einen kann die subjektive Wahrscheinlichkeit nun nicht mehr von der objektiven abweichen.[31] Zum zweiten können alle Entscheidungsprobleme unter Unsicherheit auf das Problem reduziert werden, ein Präferenzfunktional für die Ergebnismatrix $E = \begin{pmatrix} p_1, p_2, \ldots, p_S \\ w_{a1}, w_{a2}, \ldots, w_{aS} \end{pmatrix}$ der Handlung a zu finden, wobei es sich bei den unterstellten Eintrittswahrscheinlichkeiten p_{aS} um objektive Wahrscheinlichkeiten handelt. Schließlich ermöglicht dieses Vorgehen die Anwendung der mathematischen Wahrscheinlichkeitsrechnung[32], welche besonders für die Ermittlung ökonomischer Effizienzkriterien eine geeignete Grundlage liefert.

Nachdem die Problematik subjektiver Wahrscheinlichkeiten entschärft wurde, ist es dennoch notwendig, den Begriff der objektiven Wahrscheinlichkeit genauer zu untersuchen. Unter objektiver Wahrscheinlichkeit wird der Wert verstanden, der gegen die relative Häufigkeit eines Ereignisses konvergiert, wenn die Entscheidungssituation unter identischen Bedingungen wiederholt wird. Dies setzt voraus, daß sich die Informationslage vor jeder Entscheidung nicht verändert. Zwei Indivi-

---

[30] Vgl. dazu Sinn (1980), S. 14 und die dort angebenen Autoren, welche diese Vorgehensweise entwikkelten.

[31] Falls die Individuen es dennoch tun, spricht man von irrationalem Verhalten. Siehe dazu Abschnitt 1.3.1.

[32] Grundlage der mathematischen Wahrscheinlichkeitstheorie sind die folgenden von Kolmogoroff (1933) aufgestellten Wahrscheinlichkeitsaxiome: 1. Die Wahrscheinlichkeit eines Ereignisses ist eine eindeutig bestimmte, reelle, nichtnegative Zahl. 2. Diese Zahl liegt zwischen null (= unmögliches Ereignis) und eins (= sicheres Ereignis). 3. Schließen sich zwei Ereignisse aus, dann ist die Wahrscheinlichkeit für das Auftreten irgendeines Ereignisses aus dieser Menge gleich der Summe der Einzelwahrscheinlichkeiten dieser Ereignisse.

duen haben also bezüglich einer Situation nur dann die gleichen objektiven Wahrscheinlichkeiten, wenn sie die gleichen Vorinformationen besitzen.[33]

Nach dem Grad der Bekanntheit der Wahrscheinlichkeiten bzw. der Informiertheit der Entscheidungsträger über die relativen Häufigkeiten der interessierenden Ereignisse lassen sich folgende Arten von Entscheidungssituationen differenzieren:[34]

Neben der Konstellation, in der die Wahrscheinlichkeiten mit Sicherheit bekannt sind, zählt Sinn auch die Verhältnisse mit völlig bekannten Wahrscheinlichkeitshierarchien[35] zur Kategorie Risiko. Unter Ungewißheit teilt er zum einen Situationen mit nur teilweise bekannten Wahrscheinlichkeitshierarchien und zum anderen Zustände mit völlig unbekannten Wahrscheinlichkeiten ein.

Ein Entscheidungsproblem läßt sich am einfachsten analytisch handhaben, wenn objektive Wahrscheinlichkeiten mit Sicherheit vorliegen. Jedoch ist dies in der Realität und deshalb auch in unserem Zusammenhang i. d. R. nicht der Fall. Mit Hilfe von Gedankenexperimenten ist es aber möglich, die drei restlichen Fälle auf den Risikofall sicher bekannter objektiver Wahrscheinlichkeiten zu überführen.[36]

Im weiteren Vorgehen wird also von objektiven, mit Sicherheit bekannten Wahrscheinlichkeitsverteilungen ausgegangen. Diese Annahme ermöglicht zum einen die Ableitung optimaler Präventionsmaßnahmen und Versicherungsentscheidungen nach der Erwartungsnutzenregel und ist zum anderen notwendig für die Bildung eines Referenzrahmens, der zur Ableitung von Allokationsineffizienzen im Bereich der Schadenverhütung bzw. der Produktsicherheit benötigt wird.

1.2.2.3 Entscheidungsregeln unter Unsicherheit

In der fünften Prämisse wird den Individuen unterstellt, daß sie unter Unsicherheit nach einer bestimmten Entscheidungsregel zwischen den ihnen möglichen Hand-

---

[33] Aus diesem relativ häufigen Sachverhalt kann also bereits eine asymmetrische Informationsverteilung über Schadeneintrittswahrscheinlichkeiten resultieren.

[34] Zur erstmaligen begrifflichen Unterscheidung von Risiko und Unsicherheit vgl. Knight (1921) S. 20. Die folgende Differenzierung geht auf Sinn (1980), S. 22, zurück.

[35] Sinn (1980), S. 22, versteht unter dem Begriff Wahrscheinlichkeitshierarchien, daß „alternative Wahrscheinlichkeitsverteilungen über den Zuständen der Welt für möglich gehalten werden, hierfür unter Umständen selbst wieder alternative Wahrscheinlichkeitsangaben zu berücksichtigen sind".

[36] Dieses Vorgehen wird als Luce-Raiffa-Schlaifer-Ansatzes bezeichnet. Vgl. zu der Analyse der einzelnen Fälle Sinn (1980), S. 23-47.

lungsalternativen entscheiden. Unter Sicherheit besteht das Entscheidungsproblem darin, eine Zielvariable - sei es Gewinn oder Nutzen - zu maximieren. Unter Unsicherheit wird das Entscheidungsproblem durch die Varianz der Konsequenzen mehrdimensionaler, so daß eine Reihe zwei-parametrisch-substitutionaler Kriterien entwickelt wurde, deren bekanntestes das in der Portfoliotheorie angewandte $\mu-\sigma$-Kriterium ist.[37] Eine ähnliche Struktur haben lexikographische Zielfunktionen, welche eine Variable unter Beachtung verschiedener Nebenbedingungen zu maximieren versuchen.[38]

Zur weiteren Analyse der individuellen Entscheidung über Sicherheitsvorkehrungen wird hier das von Morgenstern und von Neumann entwickelte Erwartungsnutzenkriterium herangezogen, nach welchem das Wirtschaftssubjekt die Handlungsalternative auswählen wird, die den höchsten Erwartungswert des Nutzen erbringt.

1.2.2.4 Die Erwartungsnutzenfunktion

Nach den Prämissen drei und vier können die Individuen zum einen den Konsequenzen w_{aS} ihrer Handlungsalternativen a unter den verschiedenen Zukunftskonstellationen monetäre Vermögenswerte zuordnen und zum anderen diesen Größen wiederum Nutzenwerte beimessen. Deshalb stellt eine Reihung der Konsequenzen nach ihrer Gewünschtheit für den Entscheidenden kein Problem dar, wenn unterstellt wird, daß höhere Vermögenswerte einen größeren Nutzen stiften. Die Schwierigkeit besteht nun darin, die Intensität der Präferenzen für die verschiedenen Handlungsalternativen zu bestimmen und zu reihen, damit es möglich wird, die optimale Handlungsalternative auszuwählen.[39]

Die Verbindung zwischen den Präferenzen bezüglich der Konsequenzen w_{aS} und den Nutzen der verschiedenen Handlungsalternativen wurde erstmals durch das Erwartungsnutzenkonzept von von Neumann und Morgenstern geschafft.[40] Nach

---

[37] Vgl. dazu die Übersicht in Sinn (1980), S. 51, und seine genaueren Ausführungen auf Seite 53-66.

[38] Vgl. ebenda S. 66-78.

[39] Vgl. dazu Hirshleifer & Riley (1992), S. 13.

[40] Vgl. dazu den originären Beitrag von von Neumann & Morgenstern (1944), S. 15-31, und die Darstellungen in Sinn (1980), S. 78-89, und Hirshleifer & Riley (1992), S. 14-19, welche als Grundlage für diesen Abschnitt dienen. Auf die axiomatische Darstellung des Erwartungsnutzenkonzeptes wird hier verzichtet. Vgl. dazu Sinn (1980), S. 89-95, und Hirshleifer & Riley (1992), S. 19f.

dem Erwartungsnutzentheorem wird das Wirtschaftssubjekt die Handlungsalternative a wählen, bei welcher der Erwartungswert des Nutzens maximal ist:[41]

$$(1) \qquad \max_{a} E[U(w_a)] = \max_{S} \sum p_s \cdot U(w_{aS}).$$

Gleichung (1) drückt aus, daß der Erwartungsnutzen einer Handlungsalternative $E[U(w_a)]$ gleich dem Erwartungswert bzw. dem wahrscheinlichkeitsgewichteten Durchschnitt der elementaren Nutzen $U(w_{aS})$ der entsprechenden Konsequenzen w_{aS} ist. Es handelt sich also um eine lineare Transformation der Nutzenfunktion $U(w_{aS})$.[42]

Die Funktion $U(w_{aS})$ bezieht sich auf eine kardinale Skala. Eine kardinale Variable ist quantitativ bestimmbar und auf einer Intervallskala meßbar.[43] Dagegen handelt es sich bei $E[U(w_{aS})]$ um eine ordinal meßbare Variable. Deshalb gilt folgendes: Ordnet eine Präferenzordnungsfunktion $U(w_{aS})$ den Konsequenzen eine kardinale Nummer zu, dann wird eine ordinale Transformation $E[U(w_a)]$ nichts an der Ordnungsreihenfolge ändern. Bei Sicherheit muß diese Transformationsfunktion nur eine positive erste Ableitung aufweisen, während unter Unsicherheit die Transformationsfunktion zusätzlich linear sein muß, damit sich die Ordnungsreihenfolge nicht verändert.

Um etwas über das Verhalten eines Individuums bei Unsicherheit aussagen zu können, muß schließlich seine Einstellung gegenüber dem Risiko, d. h. der Streuung der Vermögensverteilung, bestimmt werden. Gewöhnlich wird den Wirtschaftssubjekten Risikoaversion unterstellt, welche wie folgt definiert ist: Eine Person gilt als risikoavers, wenn sie ein sicheres Vermögen einem unsicheren Vermögen vorzieht, dessen Erwartungswert dem der sicheren Konsequenz entspricht. Falls sie dagegen die risikoreiche Alternative vorzieht, dann ist sie ein "risk-preferrer" oder "risk-

---

41 Nach Sinns Terminologie besteht der Erwartungsnutzenansatz darin, mit Hilfe einer Nutzenfunktion $U(w_{aS})$ die Wahrscheinlichkeitsverteilung über die Endvermögenswerte der Konsequenzen w_{aS} in eine solche über Nutzenwerte umzuwandeln und dann den Erwartungswert davon zum Präferenzfunktional bzw. zur Bewertungsregel zu wählen. Vgl. dazu Sinn (1980), S. 78.

42 Außerdem berührt eine Konsequenz w_{aS}, realisiert in einem Zustand S, auf keinen Fall die Präferenzenordnung $U(w_{aS^o})$ in einem anderen Zustand S°. D. h. es existieren keine Interdependenzen zwischen der Bewertung der Konsequenzen in den einzelnen Zuständen.

43 Kardinale Variablen haben die Eigenschaft, daß unabhängig von der Verschiebung des Nullpunktes und der Änderung des Einheitsintervalls die relative Größe von Differenzen konstant bleibt. Vgl. dazu Hirshleifer & Riley (1992), S. 14. Vgl. zur Problematik des kardinalen Nutzenkonzeptes Sinn (1980), S. 86f.

lover". Ist sie indifferent zwischen den beiden Alternativen, dann gilt sie als risikoneutral.

Bezogen auf die Nutzenfunktion $U(w_{aS})$ bedeutet Risikoaversion die Gültigkeit des ersten Gossenschen Gesetzes oder eine konkave Nutzenfunktion ($U''(w_{aS})<0$).[44] Graphisch wird dies anhand Abbildung 1 deutlich, welche eine Zwei-Punkt-Vermögensverteilung mit einem Normalfall (Ausgangsvermögen $w_{11}=W$) und einem Schadensfall (Restvermögen $w_{12}=W-L$), der mit der Schadenswahrscheinlichkeit p eintritt, illustriert:

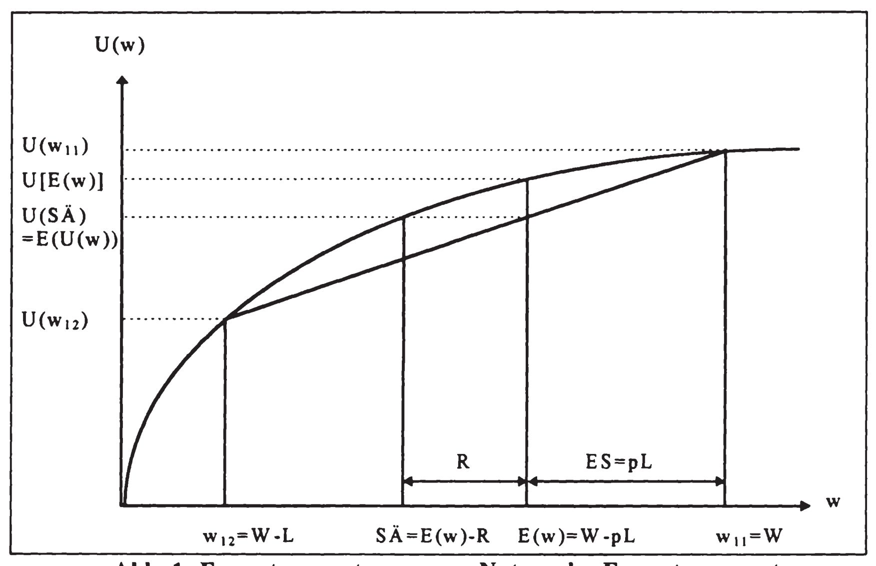


Abb. 1: Erwartungsnutzen versus Nutzen des Erwartungswertes

Aus der Konkavität[45] der Nutzenfunktion leitet sich für die Erwartungsnutzenfunktion des angebenen Szenarios folgendes ab:

$$(2) \qquad pU(w_{12})+(1-p)U(w_{11})=E\left[U(w_1)\right]<U\left[E(w_1)\right]=U(W-pL).$$

Vor dem Hintergrund der Zielfunktion von Gleichung (1) läßt sich daraus ablesen, daß ein risikoaverses, nutzenmaximierendes Individuum ein sicheres Vermögen in

[44] Mit Apostrophen versehene Funktionen repräsentieren deren erste bzw. weitere Ableitungen.

[45] Die Begriffe Konkavität, Konvexität und Linearität einer Funktion definiert man dadurch, daß man den Funktionswert einer beliebigen Linearkombination von Argumenten mit der entsprechenden Linearkombination der Funktionswerte selbst vergleicht. Vgl. dazu Sinn (1980), S. 79f.

Höhe des Erwartungswertes einer stochastischen Verteilung von Vermögenswerten vorzieht und sogar bereit ist, für die Beseitigung der zufälligen Vermögensstreuung zusätzlich zum Erwartungsschaden (ES=pL) bis maximal die Risikoprämie R auszugeben.[46] Denn bis zum Grenzfall des Sicherheitsäquivalentes SÄ liegt der daraus resultierende sichere Nutzen über dem Erwartungsnutzen der zufälligen Vermögensstreuung. Dies bildet die notwendige Grundlage für das weitere Vorgehen. Denn auf dieser positiven Zahlungsbereitschaft für den Schutz vor Vermögensrisiken gründet sich die Nachfrage nach Schadenpräventionsmaßnahmen und Versicherungen.[47]

Deshalb ist auch die Intensität der Riskoaversion von Interesse, weil sie das Ausmaß der Nachfrage nach Sicherheitsmaßnahmen in Form der Risikoprämie R positiv beeinflußt. Der Grad der Risikoaversion wird i. d. R. durch die absolute Risikoaversion, definiert als $AR(w) = -\frac{U''(w)}{U'(w)}$, quantitativ bestimmt.[48] Sie drückt die Intensität der Risikoaversion in Abhängigkeit des Vermögenswertes w aus, wobei mit steigender Risikoscheue der Wert von AR(w) zunimmt. Mit Bezug auf Abbildung 1 führt eine intensivere Risikoaversion zu einer stärkeren Krümmung der Nutzenfunktion U(w) und damit c. p. auch zu einer höheren Risikoprämie R.

Im weiteren Verlauf der Analyse wird eine konkave Nutzenfunktion U(w) angenommen bzw. wird davon ausgegangen, daß die Individuen in der Regel risikoavers sind und fallende Grenznutzen aus zusätzlichem Vermögen oder Einkommen haben und deshalb ihre absolute Risikoaversion immer positiv ist.[49] Das bedeutet, daß

---

[46] Der subjektive Risikopreis R ist als die Differenz zwischen dem Erwartungswert der monetären Werte w_{aS} der Konsequenzen und dem Sicherheitsäquivalent, dessen Nutzen genauso hoch ist wie der Erwartungsnutzen der unsicheren Vermögensverteilung, definiert. Vgl. dazu Schulenburg (1993), S. 536.

[47] Ein positiver Grenznutzen der Schadensprävention ergibt sich für risikoneutrale Individuen bereits dann, wenn sich der Erwartungswert W-pL durch den Aufwand einer Einheit an Präventionsmaßnahmen marginal erhöht.

[48] Dieses Maß wurde von Arrow (1965) und Pratt (1964) entwickelt. Außerdem wird in der Literatur die relative Risikoaversion, definiert als die Elastizität $\frac{\partial U'(w) / \partial w}{U'(w) / w}$, herangezogen. Vgl. den Überblick verschiedener Definitionen von Risikoaversion Heinlin (1993), S. 33-57.

[49] In der Literatur wird i. d. R. von abnehmender absoluter Risikoaversion ausgegangen, da zum einen dies dem individuellen Entscheidungsverhalten bei Ungewißheit am nächsten kommt und zum anderen sich dadurch ähnliche Resultate wie bei Entscheidungen unter Sicherheit ergeben. Vgl. dazu Quiggin (1992), S. 44.

risikofreudige Individuen und weitere Entscheidungsparadoxons bei Unsicherheit ausgeschlossen werden.[50]

1.2.3 Die optimale Allokation verschiedener Sicherheitsstrategien bei potentiellen Schadensfällen

Nachdem in den vorangegangenen Abschnitten die Prämissen festgelegt und die Verhaltensweisen der Wirtschaftssubjekte bei Unsicherheit charakterisiert wurden, wird in diesem Abschnitt ein repräsentatives und einfaches Szenario beschrieben, welches die Situation eines Individuums darstellt, das mit positiven Schadenswahrscheinlichkeiten konfrontiert wird. Hierunter kann man sich vorstellen, daß durch den Gebrauch von Produktions- oder Konsumgütern Schadensfälle auftreten können.[51] Es sind in diesem vereinfachten Modellrahmen nur zwei zukünftige Zustände S=1,2 möglich, welche jeweils mit den Wahrscheinlichkeiten 1-p bzw. p eintreten können. Zustand 1 ist der „Normalfall", in dem bei der Nutzung der Güter kein Schaden eintritt und das Individuum sein Ausgangsvermögen W behält. Umgekehrt fällt im Zustand 2, welcher mit der Wahrscheinlichkeit p eintreten kann, ein Schaden in Höhe von L an, welcher das ursprüngliche Vermögen W reduziert. Deshalb wird p auch als Schadeneintrittswahrscheinlichkeit bezeichnet.[52] Es werden in den folgenden Abschnitten die Handlungsalternativen a von zwei bis fünf behandelt und jeweils die optimale Nachfrage nach Präventionsmaßnahmen abgeleitet. Zur übersichtlichen Illustration dient Übersicht 1 über die Vermögenssituationen, wenn verschiedene Handlungsalternativen ergriffen werden:[53]

---

[50] Entscheidungen unter Unsicherheit, welche nicht risikoaversem Verhalten entsprechen, werden als irrational bezeichnet. Vgl. dazu Hirshleifer & Riley (1992), S.33-39, und Abschnitt 1.4.1.

[51] Voraussetzung dafür, daß ein risikobehaftetes Gut überhaupt erworben bzw. benutzt wird, ist ein trotz Verlustgefahren positiver Erwartungsnutzen. Falls dies nicht der Fall ist, wird die risikobhaftete Aktivität unterlassen bzw. das Produkt nicht gekauft. Es wird also angenommen, daß $E[U] = (1-p)U(W) + pU(W-L) \geq 0$ gilt.

[52] Die Schadeneintrittswahrscheinlichkeit p kann auch als der Prozentsatz defekter Konsum- bzw. Produktionsgüter angesehen werden. In der weiteren Analyse wird p jedoch als der prozentuelle Anteil der Fälle verstanden, in denen es durch den Gebrauch eines funktionstüchtigen Produktes zu Schäden kommt.

[53] Eine ähnliche Darstellung findet sich in Schulenburg (1992), S. 401, oder (1993), S. 534.

Handlungsalternativen	potentielle Zustände	
	S=1 (Normalfall)	S=2 (Schadensfall)
a=1 (keine Schutzmaßnahmen)	w_{11}=W	w_{12}=W-L
Wahrscheinlichkeiten	1-p	p
a=2 (Self-protection)	w_{21}=W-C(r)	w_{22}=W-C(r)-L
Wahrscheinlichkeiten	1-p(r)	p(r)
a=3 (Self-insurance)	w_{31}=W-C(c)	w_{32}=W-C(c)-L(c)
Wahrscheinlichkeiten	1-p	p
a=4 (kombinierter Schutz)	w_{41}=W-C(s)	w_{42}=W-C(s)-L(s)
Wahrscheinlichkeiten	1-p(s)	p(s)
a=5 (Versicherung)	w_{51}=W-qdL	w_{52}=W-(1-d(1-q))L
Wahrscheinlichkeiten	1-p	p

Übersicht 1: Vermögenszustände bei verschiedenen Sicherheitsstrategien

Werden jegliche Vorsorgemaßnahmen unterlassen, berechnet sich der Erwartungsnutzen $E[U(w_1)]$ wie folgt:

$$(3) \qquad E[U(w_1)] = pU(W-L) + (1-p)U(W).$$

Der Nutzen des Erwartungswertes $U[E(w_1)]$ ist dagegen definiert als:

$$(4) \qquad U[E(w_1)] = U[p(W-L)+(1-p)W] = U[W-pL].$$

Da es sich um ein risikoaverses Individuum handelt, gilt:

$$(5) \qquad E[U(w_1)] < U[E(w_1)].$$

Wenn der Erwartungsnutzen geringer als der Nutzen des Erwartungswertes ist, dann ist es bereit, einen positiven Preis bis in Höhe von R für den Tausch seiner

stochastischen Vermögensverteilung [W, W-L] in ein sicheres Vermögen in Höhe des Sicherheitsäquivalentes SÄ zu zahlen und auch deshalb Nachfrage nach Vorsorgemaßnahmen zu entfalten. Das Individuum hat nun vier verschiedene Möglichkeiten, um durch Vorsorgemaßnahmen auf dieses mit Unsicherheit behaftete Szenario zu reagieren:[54]

1. Es kann Präventivmaßnahmen treffen, welche die Schadeneintrittswahrscheinlichkeit p reduzieren (a=2 („self protection")).

2. Es kann mit verschiedenen Mitteln daran gehen, die Schadenhöhe L zu reduzieren (a=3 („self-insurance")).

3. Es kann komplexe Präventivmaßnahmen ergreifen, welche sowohl die Schadeneintrittswahrscheinlichkeit p als auch die Schadenhöhe L reduzieren. (a=4)

4. Falls eine Versicherungsmöglichkeit existiert, kann es sich gegen den Schadensfall versichern (a=5).[55]

Es wird nun untersucht, wie sich ein rationales Wirtschaftssubjekt optimal verhält bzw. wie groß ohne Berücksichtigung der jeweils anderen Präventionsstrategien der individuelle Grenznutzen bzw. die Nachfrage nach den jeweiligen Sicherheitsmaßnahmen ist.[56]

1.2.3.1 Das optimale Ausmaß an Maßnahmen zur Reduktion der Schadenswahrscheinlichkeit: Self-protection[57]

Es wird davon ausgegangen, daß das Individuum der oben angegebenen Ausgangssituation dadurch begegnen kann, indem es Maßnahmen zur Reduktion der Schadenswahrscheinlichkeit ergreift. Nun gilt es, ein Maximierungskalkül hinsichtlich des Erwartungsnutzens aufzustellen, um das optimale Niveau der Aufwendungen für eine Reduktion der Schadenswahrscheinlichkeit p bestimmen zu können. Das Individuum kann die Maßnahme r, dessen Gesamtkosten C(r) mit $C'(r)>0$ in

---

[54] Vgl. dazu den Beitrag von Ehrlich & Becker (1972) und weitere Risikovermeidungsstrategien in Schulenburg (1993), S. 538.

[55] Zunächst wird unterstellt, daß ein privates Versicherungsangebot existiert.

[56] Substitutions- und Komplementaritätsbeziehungen werden zunächst unberücksichtigt gelassen.

[57] Dieser Abschnitt bezieht sich im wesentlichen auf den Beitrag von Ehrlich & Becker (1972), S. 637ff, welche diese Art von Schutzmaßnahmen als „self-protection" bezeichnen.

Geldeinheiten gemessen werden, für eine Reduktion der Schadeneintrittswahrscheinlichkeit p ergreifen. Ein Beispiel für eine solche Vorsorge ist der Einbau einbruchssicherer Schlösser, die die Zahl erfolgreicher Einbrüche vermindern kann. Die Folge dieser Art von Vorsorge ist keine Einkommensumverteilung weg vom Nichtschadensfall hin zum Schadensfall, sondern eine „Wahrscheinlichkeitsumverteilung", die die relative Häufigkeit der Schadensfälle reduziert und die der Nichtschadensfälle erhöht. Dabei gelte, daß höhere Aufwendungen zwar zu einer weiteren Reduktion der Schadeneintrittswahrscheinlichkeit führen ($p'(r)<0$), aber die Grenzproduktivität dieser Maßnahmen abnehmend sei ($p''(r)>0$).

Nach Aufwendungen in Höhe von C(r) stehen dem Individuum folgende Vermögen in den jeweiligen Situationen zur Verfügung. Im Schadensfall (Situation 2) hat es noch W-C(r)-L und im Nichtschadensfall (Situation 1) W-C(r) an Vermögen.

Die Optimierungsaufgabe des Individuums besteht nun darin, den Erwartungswert seines Nutzen durch die entsprechende Wahl der Aufwendungen r, welche die Schadeneintrittswahrscheinlichkeit p reduzieren, zu maximieren:

$$(6) \qquad \max_r E\left[U(w_2)\right] = \max_r \left[p(r)U(w_{22}) + (1-p(r))U(w_{21}))\right].$$

Durch Differenzieren nach r erhält man folgende Bedingung erster Ordnung:

$$(7) \qquad \begin{aligned} &p'(r)U(w_{22}) + p(r)U'(w_{22})(-C'(r)) + \\ &((-p'(r))U(w_{21}) + (1-p(r))U'(w_{21})(-C'(r)) \overset{!}{=} 0 \end{aligned}$$

$$\text{bzw.: } (7') \quad MB_r = \frac{-p'(r^*)\left(U(w_{21}) - U(w_{22})\right)}{(1-p(r^*))U'(w_{21}) + p(r^*)U'(w_{22})} = C'(r^*).$$

Der Term auf der linken Seite der Gleichung drückt den durch eine Reduzierung der Schadeneintrittswahrscheinlichkeit ausgelösten marginalen Nutzengewinn MB_r aus, während diesem auf der rechten Seite die Grenzkosten gegenüberstehen. Im Optimum r* müssen sich Grenznutzen und Grenzkosten ausgleichen.[58]

---

[58] Für ein Erwartungsnutzenmaximum muß die zweite Ableitung negativ sein. Dies ist auch bei endlicher Risikoaversion immer der Fall. Vgl. dazu Ehrlich & Becker (1972), S. 639, und Nell (1993), S. 72.

Über eine komparativ-statische Analyse können die Bestimmungsgründe der optimalen Aufwendungen zur Reduzierung der Schadeneintrittswahrscheinlichkeit ermittelt werden.

Zunächst wird die partielle Ableitung des Grenznutzens MB_r nach der Schadenhöhe L gebildet, um zu bestimmen, ob mit steigender Schadenhöhe L r* zu- oder abnimmt:

$$(8) \quad \frac{\partial MB_r}{\partial L} = \frac{-p'(r^*)U'(w_{22})\left[(1-p(r^*))U'(w_{21})+p(r^*)U'(w_{22})\right]}{\left[1-p(r^*))U'(w_{21})+p(r^*)U'(w_{22})\right]^2} - \frac{p'(r^*)(U_{21}-U_{22})p(r^*)U''(w_{22})}{\left[1-p(r^*))U'(w_{21})+p(r^*)U'(w_{22})\right]^2}.$$

Da der Nenner eindeutig positiv ist, muß für die Zähler folgende Bedingung gelten, damit eine Erhöhung der Schadenhöhe L auch zu einem Anstieg an Maßnahmen zur Senkung der Schadeneintrittswahrscheinlichkeit führt:

$$(8') \quad U'(w_{22})\left[(1-p(r^*))U'(w_{21})+p(r^*)U'(w_{22})\right] > -p(r^*)U''(w_{22})(U_{21}-U_{22}).$$

Diese Ungleichung zeigt, daß bei kleinen Schadeneintrittswahrscheinlichkeiten und einer nicht zu starken Änderung der Risikoaversion im betrachteten Vermögensintervall [W, W-L] von einem positiven Einfluß von L auf r* ausgegangen werden kann.[59]

Es wird ein positiver Einfluß der exogenen Schadenswahrscheinlichkeit auf die Produktivität der Sicherheitsmaßnahmen (∂-p´(r)/∂p>0) unterstellt, was durchaus realistisch ist, wenn man bedenkt, daß in einem Szenario mit hohen Schadenswahrscheinlichkeiten einfache und kostengünstige Maßnahmen ihre Wirkung viel effizienter entfalten können als in gefahrlosen Umgebungen. Vor dem Hintergrund dieser Prämisse kommt man hinsichtlich des Einflusses der Veränderung der Schadeneintrittswahrscheinlichkeit p auf den Grenznutzen MB_r zu folgendem Ergebnis:

[59] Vgl. dazu auch die Ergebnisse der formalen Analyse von Sweeney & Beard (1992), S.307f. Zu qualitativ denselben Ergebnissen kommen auch Briys & Schlesinger (1990) und Dionne & Eeckoudt (1985), die die Analyse anhand unterschiedlich spezifizierter Nutzenfunktionen illustrieren.

(9)
$$\frac{\partial MB_r}{\partial p} = \frac{-\partial p'(r)/\partial p[U(w_{21}) - U(w_{22})]}{[(1-p(r^*))U'(w_{21}) + p(r^*)U'(w_{22})]} + \frac{p'(r^*)[U(w_{21}) - U(w_{22})][U'(w_{22}) - U'(w_{21})]}{[(1-p(r^*))U'(w_{21}) + p(r^*)U'(w_{22})]^2}.$$

Für risikoneutrale Individuen ist $\partial MB_r/\partial p$ immer größer null, weil aufgrund der Risikoneutralität der zweite Term gleich null ist, während der erste eindeutig ein positives Vorzeichen hat. Dagegen erhöhen risikoaverse Wirtschaftssubjekte ihre Self-protection-Aktivitäten nur dann, wenn folgende Bedingung erfüllt ist:

(9')
$$-\partial p'(r^*)/\partial p[(1-p(r^*))U'(w_{21}) + p(r^*)U'(w_{22})] > -p'(r^*)[(U'(w_{22}) - U'(w_{21})].$$

Interpretiert man diese Ungleichung, kommt man zu dem Ergebnis, daß die Erhöhung der Grenzproduktivität von r durch ∂p multipliziert mit einem Term, der den durchschnittlichen Grenznutzen repräsentiert, stärker ausfallen muß als die marginale Erhöhung der Differenz zwischen den Grenznutzen in den beiden potentiellen Situationen. Ein exogener Anstieg der Schadeneintrittswahrscheinlichkeit erhöht zwar den erwarteten Schaden, jedoch kann nicht eindeutig bestimmt werden, ob das Individuum darauf mit einer Ausweitung seiner Vorsorgeaufwendungen reagiert. Es kann lediglich konstatiert werden, daß geringe Grenzproduktivität und hohe Grenzkosten, also ein ungünstiges Preis-Leistungsverhältnis, trotz steigender Schadeneintrittswahrscheinlichkeit zu einem Rückgang von Self-protection führen werden.[60]

[60] Vgl. dazu den Beweis von Nell (1993), S. 82ff, und Briys & Schlesinger (1990), S.462. Deshalb führt auch ein allgemeiner Vermögens- oder Einkommensanstieg nur unter bestimmten Bedingungen zu einer Nachfragesteigerung nach Maßnahmen zur Schadeneintrittswahrscheinlichkeitenverminderung. Hier ist auch die Veränderung der durchschnittlichen Risikoaversion über das Intervall [W, W-L] entscheidend dafür, ob mehr oder weniger Vorsorge getroffen wird, wenn W steigt. Vgl. dazu Sweeney & Beard (1992), S. 303-307.

Sinkt schließlich die Grenzproduktivität der Schadeneintrittsverminderungsmaßnahmen, wird sich der Grenznutzen vermindern und das Individuum wird seine Aufwendungen für r einschränken, weil gilt:[61]

$$(10)\quad \frac{\partial MB_r}{\partial p'(r^*)} = \frac{-(U(w_{21}) - U(w_{22}))}{(1-p(r^*))U'(w_{21}) + p(r^*)U'(w_{22})} < 0.$$

Hinsichtlich der Risikoaversion kann keine eindeutige Aussage gemacht werden. Der Grund liegt darin, daß es einen Schwellenwert für die Schadeneintrittswahrscheinlichkeit gibt, nach dessen Erreichen die Zahlungsbereitschaft für eine Verringerung der Eintrittswahrscheinlichkeit zurückgeht. Dies liegt darin begründet, daß höhere Aufwendungen für r nicht die absolute Vermögensstreuung reduzieren. Besonders bei hohen Schadenswahrscheinlichkeiten kann der Einfluß des Grades der Risikoaversion auf die Höhe von r nicht eindeutig bestimmt werden.

Sowohl die Grenzkosten - die rechte Seite der Optimalitätsbedingung von Gleichung (7′) - als auch die Grenznutzen - die linke Seite von Gleichung (7′) sind in Abbildung 2 als Funktionen von r abgetragen. Der Grenznutzen fällt durch die unterstellte abnehmende Grenzproduktivität der Self-protection-Maßnahmen.

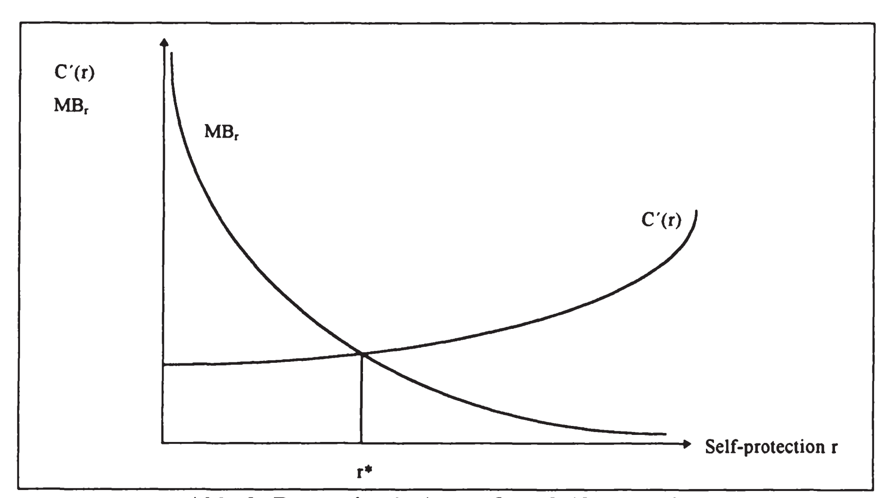


Abb. 2: Das optimale Ausmaß an Self-protection

[61] Zu diesem Ergebnis kommt auch Hiebert (1983), S. 167, der das Niveau an Self-protection für ein Unternehmen bei vollkommener Konkurrenz untersucht, wobei Einkommenseffekte ausgeschlossen werden.

Die vorangegangene Analyse hat gezeigt, daß zwar Konstellationen existieren, welche zu anomalen Reaktionen führen können. Unterstellt man aber relativ effiziente Self-protection-Maßnahmen, dann hängt das optimale Ausmaß an Schadeneintrittsverminderungsmaßnahmen r von den betrachteten Faktoren wie folgt ab:

$$(11) \quad r^* = r^*(\underset{+}{L}, \underset{+}{p}, \underset{-}{p'(r)}, \underset{?}{AR(w)}).$$

Im folgenden Abschnitt wird dieselbe Vorgehensweise hinsichtlich der Mechanismen zur Reduktion der Schadenhöhe angewandt.

1.2.3.2 Das optimale Ausmaß an Schadenbegrenzungsmaßnahmen: Self-insurance

Neben der Vorsorge, die sich auf die Reduzierung der Schadeneintrittswahrscheinlichkeit bezieht, steht den Wirtschaftssubjekten i. d. R. auch die Möglichkeit offen, Maßnahmen zur Begrenzung der Schadenhöhe zu ergreifen.[62] Als Beispiel für eine Maßnahme, die im Schadensfall die Schadenhöhe reduziert, bietet sich die Installation einer Sprinkleranlage an, welche bei Ausbruch eines Feuers zur Schadenbegrenzung beitragen kann.

Die Ausgangssituation sei wie folgt: Der Schaden- und der Nichtschadensfall können mit den oben genannten Wahrscheinlichkeiten p und 1-p eintreten. Das Individuum kann Vorsorgemaßnahmen c treffen, welche die Schadenhöhe L im Schadensfall reduzieren. Jedoch verursacht eine Reduktion von L Kosten in Höhe von C(c) mit $C'(c)>0$. Bezüglich der Produktivität von c gelte zum einen, daß mit steigendem c die potentielle Schadenhöhe L abnimmt ($L'(c)<0$), und zum anderen, daß die Grenzproduktivität von c bzgl. der Schadenhöhe mit steigenden Werten sinkt ($L''(c)>0$). Dementsprechend verbleiben dem Individuum im Nichtschadensfall W-C(c) und im Schadensfall W-C(c)-L(c) an Vermögen.

Die Optimierungsaufgabe des Individuums besteht nun darin, den Erwartungswert seines Nutzen durch die entsprechende Wahl der Aufwendungen für Sicherheits-

[62] Dieser Abschnitt basiert auf den Ausführungen von Ehrlich & Becker (1972), S. 634-637, welche diese Art von Vorsorge als „self-insurance“ bezeichnen.

vorkehrungen in Form von c zu maximieren:

$$(12) \quad \max_{c} E[U(w_3)] = \max_{c} [pU(w_{32}) + (1-p)U(w_{31})].$$

Die Bedingung erster Ordnung für ein Optimum lautet wie folgt:

$$(13) \quad pU'(w_{32})(-L'(c) - C'(c)) + (1-p)U'(w_{31})(-C'(c)) \stackrel{!}{=} 0$$

$$\text{oder: } (13') \; MB_c = \frac{-pU'(w_{32})L'(c^*)}{pU'(w_{32}) + (1-p)U'(w_{31})} = C'(c^*).$$

Da wir einen abnehmenden Grenznutzen bezüglich des Einkommens bzw. ein risikoaverses Individuum angenommen haben und abnehmende Produktivität bzw. steigende Grenzkosten der Schadenverminderungsmaßnahmen c unterstellt haben, führt die Erfüllung der Bedingung erster Ordnung zur Maximierung des Erwartungsnutzens.[63] Die abgeleitete Optimalitätsbedingung drückt aus, daß der Grenznutzen der zuletzt eingesetzten Einheit c* gleich ihren Grenzkosten sein muß.

Für einen positiven Betrag an Schadenverminderungsmaßnahmen muß notwendigerweise mindestens gelten: $-L'(c) > C'(c)$. Dies bedeutet, daß die Aufwendung für die letzte Einheit c mindestens eine Reduktion des potentiellen Schadens L um etwas mehr als eine Einkommenseinheit bewirken muß, weil die erwartete Schadenreduktion mindestens die sicheren Schadenreduktionsausgaben ausgleichen muß.

Die statisch-komparative Analyse zur Ermittlung des Einflusses der Determinanten auf c* ergibt ohne Beachtung weiterer restriktiver Bedingungen folgende eindeutige Ergebnisse:

$$\frac{\partial MB_c}{\partial L} > 0, \quad \frac{\partial MB_c}{\partial p} > 0, \quad \frac{\partial MB_c}{\partial L'(c)} < 0.$$[64]

Sowohl ein Anstieg der potentiellen Schadenhöhe L als auch der Schadeneintrittswahrscheinlichkeit p und der Grenzproduktivität L′(c) haben einen eindeutig posi-

---

[63] Vgl. dazu Ehrlich & Becker (1972), S. 634, und Nell (1993), S. 58. Die zweite Ableitung des Maximierungsproblems ist bei risikoaversen Individuen immer negativ, so daß durch die Erfüllung der Bedingung erster Ordnung der Erwartungsnutzen auch maximiert wird.

[64] Vgl. dazu die Beweise in Ehrlich & Becker (1972), S. 635, in Nell (1993), S. 66f, oder auch die Ausführungen von Hiebert (1983), S. 164.

tiven Einfluß auf das optimale Niveau von c*. Auch eine zunehmende Risikoaversion bedingt ein höheres c*.[65]

Graphisch wird dieser Sachverhalt in Abbildung 3 dargestellt. Die Grenzkostenfunktion steigt an. Die Grenznutzenkurve fällt wegen der fallenden Grenzproduktivität von c bzgl. der Schadenhöhe L ab.

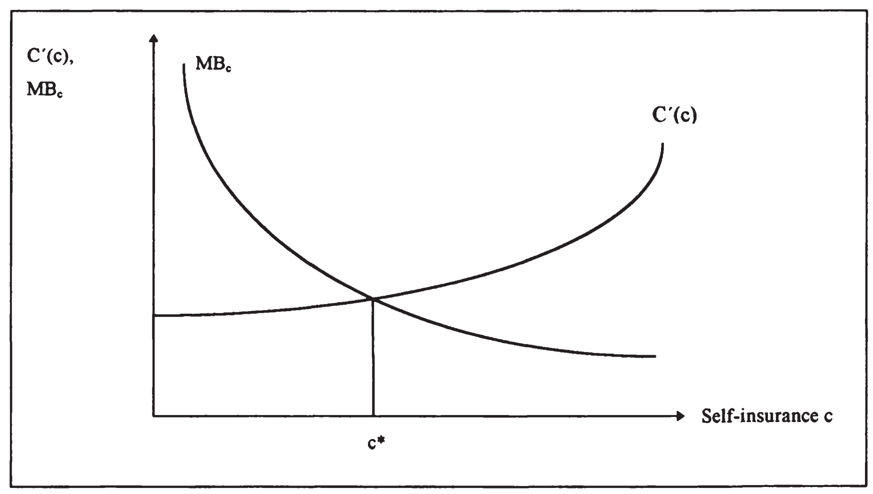


Abb. 3: Das optimale Ausmaß an Self-insurance

Das optimale Ausmaß an Schadenbegrenzungsmaßnahmen c* wird also wie folgt von den verschiedenen Determinanten bestimmt:

$$(14) \quad c^* = c^*(\underset{+}{L}, \underset{+}{p}, \underset{-}{L'(c)}, \underset{+}{AR(w)}).$$

Im Gegensatz zur Funktion r* gibt es bei den Determinanten der Funktion c* keine Fälle mit nicht eindeutigen Vorzeichen.

---

[65] Vgl. dazu die Beweise von Nell (1993), S. 59, und Briys & Schlesinger (1990), S. 460. Jedoch kann diese These bei multiplen Risikoszenarien nicht mehr aufrechterhalten werden. Vgl. dazu die Erkenntnisse von Lewis & Nickerson (1989), S. 215f, die Self-insurance bei drohenden Naturkatastrophen analysieren.

1.2.3.3 Das optimale Ausmaß an kombinierter Schadenverhütung

In den vorangegangenen Abschnitten wurde jeweils das optimale Ausmaß an Maßnahmen zur Reduktion der Schadeneintrittswahrscheinlichkeit und der Schadenhöhe bestimmt. Da in der Realität Präventivmaßnahmen im allgemeinen nicht nur auf eine Komponente des erwarteten Schadens einwirken, sondern sowohl Schadeneintrittswahrscheinlichkeit p und Schadenhöhe L beeinflussen, wird in diesem Abschnitt das optimale Ausmaß an kombinierter Schadenverhütung abgeleitet.

Gerade beim Schutz gegen kriminelle Übergriffe wird durch Maßnahmen zur Schadenbegrenzung, wie z. B. durch den Einsatz von Wachmannschaften, auch die Wahrscheinlichkeit einer Straftat gesenkt, weil die Täter eine geringere Ausbeute ihrer illegalen Aktivitäten erwarten. Umgekehrt haben Instrumente zur Senkung der Schadeneintrittswahrscheinlichkeit i. d. R. auch immer eine schadenbegrenzende Wirkung. Um diese Interdependenzen in der folgenden Untersuchung über Marktversagensgründe bzw. über staatlichen Handlungsbedarf bzgl. der Ineffizienzen auf Märkten für Sicherheitsgüter bzw. Sicherheitsmaßnahmen nicht weiter berücksichtigen zu müssen, ist es zweckmäßig, eine dritte Art von Schadenpräventionsmaßnahmen s einzuführen, welche sich dadurch auszeichnet, daß sie sowohl zur Senkung des Schadensausmaßes als auch zur Senkung der Schadeneintrittswahrscheinlichkeit beitragen kann.

In der Realität wird man außerdem mit Mehrfachrisiken konfrontiert. Falls voneinander unabhängige Schadensfälle L_1 bis L_l mit den jeweiligen Wahrscheinlichkeiten p_1 bis p_l eintreten können, dann läßt sich der erwartete Schaden, welcher mit dem Gebrauch eines Gutes oder der Nutzung eines Dienstes verbunden ist, als mit den Wahrscheinlichkeiten gewichtetes Mittel berechnen. Da eine solche komplexe Untersuchung keinen für diesen Zusammenhang relevanten Erkenntnisgewinn einbringt, wird auch von Mehrfachrisiken abstrahiert.

Analog zu den Schadenbegrenzungsmaßnahmen c und den Schadeneintrittsverminderungsvorkehrungen r wird den komplexen Schadenpräventionsgütern s unterstellt, daß durch höhere Aufwendungen s zwar sowohl die Schadeneintrittswahrscheinlichkeit als auch die Schadenhöhe sinkt ($p'(s)<0$; $L'(s)<0$), aber hinsichtlich beider Größen eine abnehmende Grenzproduktivität vorliegt ($p''(s)>0$; $L''(s)>0$).[66]

---

[66] In der Literatur unternehmen Boyer & Dionne (1983), (1989) und Chang & Ehrlich (1985) einen ähnlichen Versuch, das Problem der simultanen Optimierung der Maßnahmen zur Reduktion der

Das Entscheidungsproblem des Individuums besteht entsprechend zu den vorangegangenen Abschnitten darin, das optimale Schadenpräventionsniveau s zu bestimmen, welches seinen Erwartungsnutzen maximiert:

$$(15)\quad \max_{s} E\left[U(w_4)\right] = \max_{s}\left[(1-p(s))U(w_{41})+p(s)U(w_{42})\right]$$

Die Bedingung erster Ordnung lautet wie folgt:

$$(16)\quad \begin{aligned} &-p'(s)U(w_{41})+(1-p(s))U'(w_{41})(-C'(s))+p'(s)U(w_{42}) \\ &+p(s)U'(w_{42})(-L'(s)-C'(s))=0. \end{aligned}$$

$$\text{bzw. (16')}\quad \begin{aligned} MB_s = &\frac{-p'(s^*)(U(w_{41})-U(w_{42}))}{(1-p(s^*))U'(w_{41})+p(s^*)U'(w_{42})} \\ &+\frac{p(s^*)U'(w_{42})(-L'(s^*))}{(1-p(s^*))U'(w_{41})+p(s^*)U'(w_{42})} = C'(s^*). \end{aligned}$$

Dies bedeutet, daß der Grenznutzen MB_s der letzten Einheit s, ausgedrückt in einer marginalen Verringerung der Schadeneintrittswahrscheinlichkeit und der erwarteten Schadenmenge, gleich den Grenzkosten $C'(s^*)$ sein muß.[67]

Analog zur Ableitung der Determinanten von c* und r* könnte man durch eine partielle Ableitung des Grenznutzens auch die Vorzeichen der Determinanten von s* aus der Bedingung erster Ordnung bestimmen. Jedoch bringt die Differenzierung des komplexeren Grenznutzenterms keine befriedigenden Ergebnisse, da keine intuitive ökonomische Interpretation möglich ist und für eindeutige Vorzeichen vielfältige Restriktionen gelten müssen. Deshalb wird bei der Bestimmung der Bestimmungsfaktoren von s* auf die Ergebnisse der beiden vorangegangenen Abschnitte zurückgegriffen.

Schadeneintrittswahrscheinlichkeit und der Schadeneindämmung zu modellieren. Jedoch tritt dabei die Problematik der Substituierbarkeit bzw. der Komplementarität zwischen beiden Maßnahmen auf, welche in diesem Kontext vernachlässigt wird. Neuere Beiträge von Shogren & Crocker (1991) und Quiggin (1992) leiten Optimalitätsbedingungen vor dem Hintergrund stetiger Wahrscheinlichkeitsverteilungen ab.

[67] Für ein Erwartungsnutzenmaximum muß auch die Bedingung zweiter Ordnung erfüllt sein. Jedoch sind dazu eine Reihe komplexer Annahmen notwendig, welche sich nicht mehr intuitiv erläutern lassen. Da der quantitative Umfang der einzelnen Terme nicht bestimmt werden kann, ist nicht mit Eindeutigkeit zu bestimmen, ob die angegebene Ungleichheit gegeben ist. Es kann also sein, daß in bestimmten Fällen die Randlösung s=0 gewählt wird.

Es sind für die beiden Funktionen r* und c* jeweils die Änderung der folgenden Faktoren betrachtet worden. Neben der Schadenhöhe L und der Schadeneintritts-wahrscheinlichkeit p sind auch die jeweiligen Grenzproduktivitäten der Präventiv-maßnahmen r und c und der Grad der Risikoaversion des betrachteten Individuums nach ihren Wirkungen untersucht worden, so daß sich folgende Zusammenhänge ergeben haben:

$$(17) \quad r^* = r^*(\underset{+}{L}, \underset{+}{p}, \underset{-}{p'(r)}, \underset{?}{AR(w)})$$

$$(18) \quad c^* = c^*(\underset{+}{L}, \underset{+}{p}, \underset{-}{L'(c)}, \underset{+}{AR(w)}).$$

Zur Ableitung der Vorzeichen der Determinanten von s* werden die ermittelten Vorzeichen der beiden Funktionen r* und c* aggregiert. Die kombinierte Funktion s* kann als optimales Ausmaß an Maßnahmen zur Reduktion des erwarteten Schadens ES=pL verstanden werden, weil die Vorsorge r auf die Eintrittswahrscheinlichkeit p einwirkt und c auf die Schadenhöhe L. Die Funktion s* nimmt also folgende Form an:

$$(19) \quad s^* = s^*(\underset{+}{L}, \underset{-}{L'(s)}, \underset{+}{p}, \underset{-}{p'(s)}, \underset{+}{AR(w)}).$$

Das optimale Ausmaß an allgemeinen Schadenpräventionsmaßnahmen wird also durch die folgenden Faktoren beeinflußt.[68] Je höher die Verluste L im Schadensfall und die Schadeneintrittswahrscheinlichkeit p sind, desto umfangreicher werden die Schutzeinrichtungen sein. Mit steigender Effizienz der Sicherheitstechnik bzgl. der Reduktion von Schadenhöhe und -wahrscheinlichkeit wird auch ihr Grenznutzen zunehmen. Schließlich führt eine zunehmende absolute Risikoaversion zu einer Ausweitung des optimalen Niveaus an Sicherheitsgüter.[69]

Diese Funktion mit ihren Determinanten bildet, nachdem die besonderen Gegebenheiten des Angebots von Sicherheitsmaßnahmen untersucht worden sind, den Ansatzpunkt für die Bestimmung von Allokationsineffizienzen auf den Märkten für Sicherheitsvorkehrungen. Diese Allokationsineffizienzen können auch daraus re-

---

[68] Gleichung (19) stellt die Determinanten des Grenznutzens von bzw. der Nachfrage nach Sicherheitsgütern dar. Sie wird im folgenden sowohl als Grenznutzen- als auch als Nachfragefunktion bezeichnet, wobei letztere eigentlich auch eine Preis- bzw. Kostenkomponente enthält.

[69] Auf eine weitere graphische Darstellung wird verzichtet, da sich qualitativ dieselben Ergebnisse einstellen wie in den vorangegangenen Schaubildern.

sultieren, daß in Märkten für Substitute Fehlallokationen zu beobachten sind.[70] Deshalb wird in diesem Kapitel auch noch das First-Best-Optimum auf dem Versicherungsmarkt abgeleitet.

1.2.3.4 Das First-Best-Optimum auf dem Versicherungsmarkt

Zusätzlich zu den dargestellten Präventionsmaßnahmen besitzt das Individuum i. d. R. die Möglichkeit, sich gegen den Schadensfall zu versichern. Um Implikationen der Angebotsseite zu vermeiden bzw. um Gründe für Allokationsineffizienzen nicht vorwegzunehmen, wird in diesem Abschnitt davon ausgegangen, daß die Versicherungsanbieter dieselben korrekten Informationen wie der Versicherungsnachfrager über Schadeneintrittswahrscheinlichkeit und Schadenhöhe haben und sich risikoneutral verhalten.

Die Versicherungslösung hat qualitativ die gleichen Konsequenzen wie Maßnahmen zur Reduktion der Schadenhöhe, weil es in beiden Fällen zu einer Einkommensumverteilung weg vom Nichtschadensfall hin zum Schadensfall kommt. Das bedeutet, falls der Schadensfall eintritt, bekommt das Individuum je nach Ausgestaltung des Versicherungsvertrages für einen Teil bzw. für den gesamten Schaden L eine Kompensation K in Höhe von K=dL von der Versicherung. Der Prozentsatz d wird als Deckungsgrad bezeichnet. Andererseits muß es in jedem Fall der Versicherung eine Prämie P=qK bezahlen, welche davon abhängt, wieviel Prozent des Schadens L es im Schadensfall erstattet bekommt. Handelt es sich um eine akzentuarisch faire Prämie[71], dann entspricht q der Schadeneintrittswahrscheinlichkeit p, und die Versicherung macht unter Vernachlässigung von Transaktionskosten keinen Gewinn. Zunächst wird aber angenommen, daß die Versicherung einen Aufschlag in Höhe von mu verlangt, so daß q=(1+mu)p gilt.[72]

---

[70] Die Versicherungslösung wird zunächst allgemein als Möglichkeit angesehen, sich gegen die ökonomischen Konsequenzen von Schadensfällen zu schützen. Inwieweit Substitutionsbeziehungen bestehen und welche Interdependenzen sich dadurch zwischen dem Versicherungsmarkt und dem Markt für Sicherheitsvorkehrungen ergeben, wird im Rahmen der Analyse der Allokationsineffizienzen in Abschnitt 1.3.6 behandelt.

[71] Vgl. Schulenburg (1992), S. 401.

[72] Man kann dem Aufschlag mu zwei verschiedenen Funktionen zuordnen. Zum einen kann man den einzelnen Versicherungsanbieter mit einem positiven mu eine gewisse Marktmacht einräumen, weil mu dann einen mark-up des Preises über den Grenzkosten repräsentiert. Hier wird dagegen von einer Konkurrenzsituation ausgegangen, in welcher die Versicherungsanbieter einen Gewinn von Null realisieren, und der Aufschlag mu wird von den Versicherungen dazu benutzt, auf die in Abschnitt

Deshalb ändert sich nach Abschluß einer Versicherung die Vermögenssituation des Individuums wie folgt. Im Schadensfall steht ihm dann folgendes Vermögen (w_{52}) zur Verfügung:

$$(20) \quad W - L - P + K = W - L(1 - d(1 - (1 + mu)p)).$$

Im Nichtschadensfall (w_{51}) besitzt das Individuum:

$$(21) \quad W - P = W - (1 + mu)pdL.$$

Das Maximierungsproblem des Individuums besteht nun darin, seinen Erwartungsnutzen $E[U(w_5)]$ unter Auswahl des Deckungsgrades d zu maximieren:[73]

$$(22) \quad \max_d E\left[U(w_5)\right] = \max_d \left[pU(w_{52}) + (1-p)U(w_{51})\right]$$

Die Bedingung erster Ordnung lautet:

$$(23) \quad pU'(w_{52})(1-(1+mu)p)L + (1-p)U'(w_{51})(-(1+mu)pL) \overset{!}{=} 0$$

$$\text{bzw.: } (23') \quad \frac{U'(w_{52})}{U'(w_{51})} = \frac{(1+mu)(1-p)}{1-(1+mu)p}.$$

Handelt es sich also um eine akzentuarisch faire Versicherungsprämie, d. h. ist mu=0, dann muß gelten: $U'(w_{52})=U'(w_{51})$, was einen Ausgleich der Grenznutzen bezüglich des Einkommens bedeutet. Dies impliziert, daß das Individuum eine Vollversicherung abschließen wird, damit es im Schadens- und im Nichtschadensfall das gleiche Einkommen zur Verfügung hat. Das aktuelle Einkommen entspricht in diesem Fall immer dem erwarteten Einkommen.

Erhebt die Versicherung einen Aufschlag in Höhe von mu>0, dann wird sich der optimale Deckungsgrad d reduzieren und das Individuum wird nur noch eine "Bruchteilversicherung" wünschen. Eine Aufschlagserhöhung führt aber nicht unbedingt zu einer Kürzung der gesamten Versicherungsausgaben, weil zugleich der

---

1.3.4 durch asymmetrische Informationsverteilung verursachten Moral Hazard und adverse Selektion von seiten der Nachfrager zu reagieren und dadurch einen Null-Gewinn zu erreichen.

[73] Vgl. dazu u. a. Nell (1993), S. 42-48. Der Deckungsgrad d ist der Quotient aus der Kompensation K und dem Schaden L und darf deshalb nicht unmittelbar mit den in den vorangegangenen Abschnitten Parametern r, c und s verglichen werden. Die Vergleichsbasis zu diesen Werten liefert die in Gleichung (25) bestimmte Versicherungsprämie P.

Preis für jede versicherte Schadeneinheit zunimmt, so daß die Veränderung der gesamten Versicherungsausgaben von der Preiselastizität der Versicherungsnachfrage bestimmt wird.[74]

Das Ergebnis dieser Untersuchung kann wie folgt zusammengefaßt werden: Steht einem risikoaversen Individuum die Möglichkeit offen, sich gegen den Schadensfall zu versichern, dann wird es bei einer fairen Versicherungsprämie (mu=0) eine Vollversicherung wählen.[75] Die Folge ist, daß sich sein Einkommen im Schadensfall nicht von dem unterscheidet, welches ihm im Nichtschadensfall zur Verfügung steht.

Anhand von Abbildung 4 kann die Versicherungsentscheidung auch graphisch dargestellt werden. Das Maximum des Erwartungsnutzen wird erreicht, wenn das Individuum eine Vollversicherung für eine faire Prämie in Höhe des Erwartungsschaden ES erwerben kann. Die maximale Zahlungsbereitschaft für eine Vollversicherung setzt sich jedoch aus der Summe der fairen Prämie und der subjektiven Risikoprämie zusammen.[76] Deshalb werden risikoaverse Individuen auch Vollversicherungen nachfragen, solange der Aufschlag mu kleiner als der Quotient aus R und dem Erwartungsschaden pL ist.[77] Damit ist auch dem Versicherungsanbieter eine Höchstgrenze für den Aufschlag mu vorgegeben, welche ihm den maximalen Gewinn einbringt und dem Nachfrager die Konsumentenrente einer Vollversicherung allerdings auf Null reduziert.

---

[74] Vgl. bzgl. des formalen Beweises ebenda S. 628.

[75] Bei fairen Versicherungsprämien sind auch risikoneutrale Individuen indifferent zwischen der zufälligen Vermögensverteilung und einer Vollversicherung, weil der Erwartungswert und damit der daraus gezogene Nutzen jeweils derselbe ist.

[76] Vgl. dazu auch Sinn (1980), S. 314ff, und ausführlich Heinlin (1993), Kapitel 2.

[77] Diese Beziehung läßt sich aus folgender Ungleichung ableiten: $P = (1 + mu)pL < pL + R$. Ein Individuum wird nur dann eine solche Vollversicherung wählen, wenn keine Möglichkeit zu einer Bruchteilversicherung existiert.

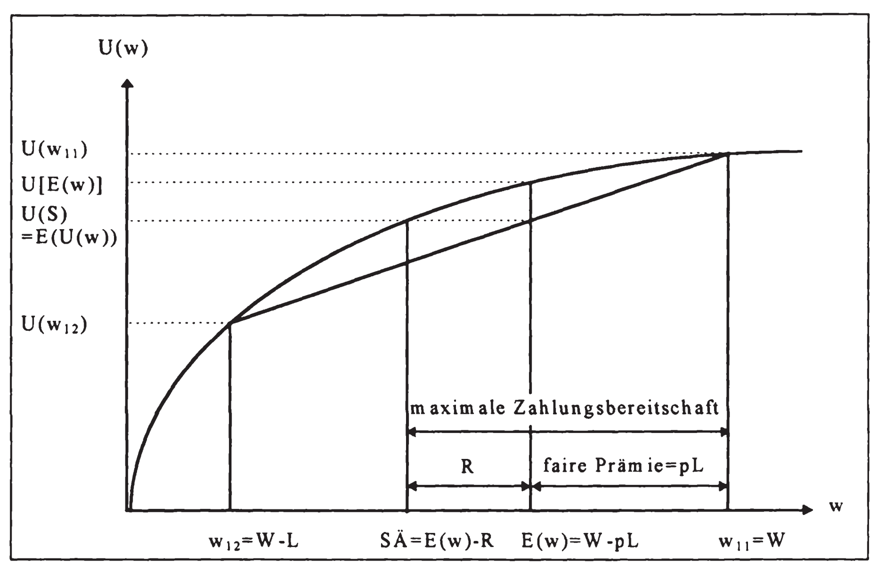


Abb. 4: Der Erwartungsnutzen bei Vollversicherung

Faßt man die Ausführungen dieses Abschnittes zusammen, sind folgende Ergebnisse festzustellen. Der gewünschte optimale Deckungsgrad hängt negativ vom Aufschlag mu ab, wobei dieser bei unvollständiger Transparenz mit der Schadenswahrscheinlichkeit p korreliert ist, weil die Versicherer damit auf Moral-Hazard-Verhalten und adverse Selektion von seiten der Versicherungsnehmer reagieren.[78] Analog zur Self-insurance wird mit steigender Risikoaversion bzw. -prämie auch ein höherer Deckungsgrad angestrebt. Im Grenzfall mu=0 wählt, wie gezeigt, jedes Individuum die vollständige Deckung seiner Schäden, d. h. d=1.

$$(24) \quad d^* = d^*(\underset{-}{mu}, \underset{+}{AR(w)}).$$

Die gezahlte Versicherungsprämie P bestimmt sich bei symmetrischer, vollständiger Informationsverteilung wie folgt:

$$(25) \quad P = (1 + mu)pdL$$

78 Aufgrund der asymmetrischen Informationsverteilung zwischen Versicherer und Versicherten wird von den Anbietern die Ausgestaltung des Aufschlages mu so gewählt, daß Verluste durch Moral-Hazard-Anreize und adverse Selektion möglichst gering gehalten werden. Auf die Interdependenzen zwischen Schadeneintrittswahrscheinlichkeit und Aufschlagshöhe wird im Rahmen der Analyse von Allokationsineffizienzen auf Versicherungsmärkten in Abschnitt 1.3.4 genauer eingegangen.

Die gesamte Versicherungsnachfrage in Form der bezahlten Prämie ist also eine positive Funktion von Schadenhöhe, Schadenswahrscheinlichkeit und gewähltem Deckungsbeitrag. Inwiefern sich eine Erhöhung von mu auf die gesamte Zahlungsbereitschaft P auswirkt, bleibt ungewiß und hängt von der Preiselastizität ab, weil der positive Effekt von mu auf die Prämie P durch eine Reduktion des Deckungsgrades d konterkariert wird. Dagegen hat der Grad der Risikoaversion bei unfairen Versicherungsprämien einen eindeutig positiven Einfluß auf die individuelle Zahlungsbereitschaft. Das Gesamtergebnis wird in Gleichung (26) zusammengefaßt:[79]

$$(26) \qquad P^* = P^*(\underset{+}{p}, \underset{+}{L}, \underset{?}{mu}, \underset{+}{AR(w)})$$

1.2.3.5 Fazit

Dieses Kapitel hat dazu gedient, die mikroökonomische Theorie der Nachfrage nach Sicherheitsgütern und -maßnahmen darzustellen und ausgehend von einem volkswirtschaftlich rational und voll informiert handelnden repräsentativen Individuum, das unter Unsicherheit nach der Erwartungsnutzentheorie entscheidet, die volkswirtschaftlichen Allokationsoptima der verschiedenen Risikovermeidungsmechanismen zu bestimmen. Dazu bedarf es zwar einer Reihe restriktiver Annahmen, jedoch ist damit ein normativer Referenzrahmen gebildet worden, der es ermöglichen wird, die verschiedenen Ursachen von Allokationsineffizienzen auf den Märkten für Sicherheitsgüter bzw. hinsichtlich der Ergreifung von Sicherheitsmaßnahmen zu identifizieren und zumindestens qualitativ zu bestimmen.

Zunächst wird im nächsten Kapitel auf Besonderheiten der Angebotsseite, für deren Preissetzung bisher die Preis=Grenzkosten-Regel unterstellt worden ist, eingegangen, bevor die zentralen Ursachen der Fehlallokation von seiten der Nachfrager untersucht werden.

---

[79] Eine differenzierte Analyse der Determinanten der Versicherungsnachfrage, einschließlich multipler Risikoszenarien, findet sich in Heinlin (1993), S. 58-93. Siehe auch Cleeton & Zellner (1993).

1.3 Besonderheiten des Angebotes an Sicherheitsgütern

1.3.1 Vorbemerkungen

Nachdem im vorangegangenen Kapitel die Allokationsoptima verschiedener Sicherheitsmaßnahmen bestimmt wurden, wobei für die Preissetzung der Angebotsseite zunächst vereinfachend Preis=Grenzkosten vor dem üblichen Hintergrund einer steigend verlaufenden Grenzkostenfunktion unterstellt wurde, besteht das Ziel dieses Kapitels darin, die Annahme dieser vereinfachten Preissetzungsregel aufzuheben, indem einige Besonderheiten der Angebotsseite herausgearbeitet werden. Die daraus folgenden Konsequenzen werden auf die Existenz von Allokationsineffizienzen untersucht.

Zuerst wird der Tatsache Rechnung getragen, daß Sicherheitsvorkehrungen in vielen risikobehafteten Produkten, in der Folge auch Basisgüter genannt, bereits integriert sind und somit Kuppelproduktion vorliegt. In diesem Fall sind sowohl Skalenerträge als auch Produktdiversifizierung möglich. Beispiele dafür sind die zahlreichen Sicherheitsausstattungen in Personenkraftwagen, wie Sicherheitsgurte, Airbags und Seitenaufprallschutz. Wenn eine separate Produktion möglich ist, dann handelt es sich um die eigenständigen Angebote verschiedener Sicherheitsgüter und -dienstleistungen. Probleme können sich hieraus durch Kompatibilitätsaspekte und Kopplungsgeschäfte („tie-in-sales") ergeben. Schließlich wird auf die Interdepedenzen von Marktversicherung und Sicherheitsmaßnahmen eingegangen und untersucht, inwieweit das Nichtzustandekommen bzw. die ineffiziente Ausgestaltung des Versicherungsangebotes durch asymmetrische Informationsverteilung Rückwirkungen auf die Nachfrage nach Sicherheitsgüter haben kann.

1.3.2 Besonderheiten der kombinierten Produktion von Basisgut und Sicherheitsmaßnahmen

Analog zu anderen Gütermärkten kann sich auch auf dem Markt für Sicherheitsgüter bzw. -dienste ein Monopol aufgrund der Subadditivität von Kostenfunktionen oder steigender Skalenerträge in der Produktion herausbilden.[80] Neben dieser all-

[80] Vgl. dazu Fritsch, Wein und Ewers (1993), S. 124-131, denn diese potentiell auf alle Güter zutreffenden Gründe für Marktineffizienzen werden hier nicht näher analysiert. Falls man eine andere Betrachtungsweise wählt, in welcher die Produktsicherheit als ein Qualitätsdimension des Konsumgu-

gemeinen Erscheinung ist in diesem Kontext die Tatsache von größerer Bedeutung, daß Sicherheitsgüter i. d. R. nicht unabhängig von den entsprechenden Produktions- oder Konsumgütern produziert werden. Sie stellen meist eine spezielle Zusatzausstattung dar, welche bereits in das Produkt integriert ist. Dadurch kann es zum einen auf der Angebotsseite zu Kostenersparnissen kommen. Zum anderen kann aufgrund individueller Präferenzen nach Sicherheitsausstattungen eine Segmentierung der Nachfrage[81] und damit eine Diversifizierung des Kuppelproduktes vorgenommen werden, welche u. U. zur Herausbildung monopolistischer Konkurrenz führen kann.

Kuppelproduktion und Economies of Scope

Die Komplementarität zwischen einem Basisgut und seinen Sicherheitsausstattungen kann ein Grund für "Economies of Scope"[82] sein, wenn durch die Kuppelproduktion ("joint production") Kostenvorteile realisiert werden können.[83] Economies of Scope liegen vor, wenn die Kosten der gemeinsamen Produktion von dem betreffenden Gut und den Sicherheitsvorkehrungen größer sind als die Summe der jeweiligen Produktionskosten des Basisgutes und der dazugehörigen Sicherheitsausstattungen. Deshalb ist es günstiger, beide Güter gemeinsam zu produzieren. Selbst wenn die jeweiligen Produktionsfunktionen separat betrachtet konstante Skalenerträge aufweisen, können bei hinreichend starken Economies of Scope in der gemeinsamen Produktion positive Skalenerträge auftreten.[84]

Liegen aufgrund der Economies of Scope Skalenerträge vor, führen diese zu fallenden Durchschnitts- und Grenzkostenverläufen des gemeinsam mit den Sicherheitsausstattungen produzierten Basisgutes. Der Anbieter wird sich nicht nach der allokationsoptimalen Preis=Grenzkosten-Regel verhalten können, sondern muß als

---

tes verstanden wird, kann der Monopolist auch über die Rationierung der Qualität seinen Gewinn maximieren und dadurch gesamtwirtschaftliche Wohlfahrtsverluste verursachen. Vgl. dazu Varian (1992), S. 239-241.

81 Die Gesamtnachfrage nach dem Basisgut teilt sich nach den unterschiedlichen Präferenzen für Sicherheitsausstattungen s auf. Vgl. bzgl. der Nachfragedeterminanten von s* Abschnitt 1.2.3.4 bzw. die Nachfragefunktion von Gleichung (19).

82 Vgl. allgemein zu "Economies of Scope" Baumol, Panzar und Willig (1988), S. 71-79.

83 Weitere in diesem Kontext nicht relevante Gründe für "Economies of Scope" können in nicht ausgelasteten Kapazitäten oder in Portfolioeffekten in der Forschung und Entwicklung begründet sein. Vgl. dazu Fritsch, Wein und Ewers (1993), S. 132, und die theoretische Darstellung in Baumol u. a (1988), S. 75-79.

84 Vgl. Baumol u. a. (1988), S. 74.

Preis mindestens die Durchschnittskosten verlangen, damit seine Kosten gedeckt werden und ihm keine negativen Gewinne entstehen.[85]

Falls der Anbieter außerdem keinen Marktzutritt von Konkurrenten befürchten muß, wird er seinen Preis für das gemeinsam produzierte Güterbündel nach der Cournot-Regel Grenzerlös=Grenzkosten setzen und damit seinen Gewinn maximieren. Dieser Monopolpreis liegt jedoch über dem nach dem Preis=Durchschnittskosten-Kriterium festgelegten Niveau und damit noch stärker über dem allokationseffizienten Preis=Grenzkosten-Level. Die Folge des über dem Grenzkostenniveau liegenden Monopolpreises ist, daß eine suboptimale Menge des Güterbündels angeboten und abgesetzt wird.

Diese Rationierung des Angebots führt zwar zu einem gesamtwirtschaftlichen Wohlfahrtsverlust, jedoch ist die gemeinsame Produktion im Sinne des Ressourcenverbrauches effizient, so daß die produktionstechnischen Vorteile der Kuppelproduktion nur im Zusammenhang mit einer Monopolsituation regulierungswürdige Ineffizienzen hervorrufen können.[86]

Produktdiversifizierung

In Kontext von Sicherheitsmaßnahmen kann sich monopolistische Konkurrenz[87] dadurch ergeben, daß die Anbieter, welche sich eigentlich einer Situation vollkommener Konkurrenz gegenübersehen, durch die Aufteilung der Gesamtnachfrage nach verschiedenen Präferenzen für Sicherheitsmaßnahmen einen Preissetzungsspielraum erhalten.[88] Da keine Marktzutrittsbarrieren existieren, wird durch den Eintritt von Anbietern weiterer bzgl. der Sicherheitsausstattung diversifizierter Basisprodukte jedoch dafür gesorgt, daß trotz einer Preissetzung nach dem Grenzkosten=Grenzerlös-Kalkül auf Dauer keine positiven Gewinne entstehen können.

---

[85] Vgl. zur Preissetzung bei fallenden Grenzkostenverläufen die Darstellung in Fritsch, Wein und Ewers (1993), S. 134-141.

[86] Die durch Kuppelproduktion möglichen Skalenerträge sind auch deshalb zu vernachlässigen, weil die Kosten der Sicherheitsausstattung an den Gesamtkosten i. d. R. nur einen kleinen Anteil ausmachen. Vgl. z. B. das Verhältnis der Kosten für die Sicherheitsgurte zu den Kosten eines kompletten Automobils.

[87] Vgl. allgemein zur monopolistischen Konkurrenz u. a. Hirshleifer & Glazer (1992), S. 242-247.

[88] Vgl. dazu die Ausführungen bzgl. Transportsicherheit von Panzar & Savage (1989), S. 38. Nell (1993), S. 171f, stellt fest, daß Reparaturmärkte, welche sich auf die ex-post-Behebung von Schäden konzentrieren, die Eigenschaften monopolistischer Konkurrenzmärkte aufweisen. Da Märkte für Sicherheitsmaßnahmen ähnliche Eigenschaften - wie Inhomogenität des Angebotes und Qualitätsunsicherheit von seiten der Nachfrage - haben, kann daraus durchaus geschlossen werden, daß sich auch hier monopolistische Konkurrenz einstellen kann.

Eine solche Situation bietet also keine Grundlage für potentielle Allokationsineffizienzen.[89]

Liegen dagegen Skalenerträge in der Produktion vor[90] und fließt in die Gesamtwohlfahrt auch das Ausmaß der Produktvielfalt ein, dann besteht gesamtwirtschaftlich ein Trade-off zwischen der vollständigen Ausschöpfung der Skalenerträge und der möglichen Produktvielfalt.[91] Es wird sich deshalb ein Marktgleichgewicht der Art einstellen, daß von einem Gut verschiedene Versionen mit unterschiedlichen Sicherheitsausstattungen angeboten werden, wobei das Ausmaß der Produktvielfalt und die Ausschöpfung von Skalenerträgen von den Präferenzen der Nachfrager bestimmt werden.

Die durch Economies of Scope und monopolistische Konkurrenz verursachten Besonderheiten des Angebotes an Sicherheitsmaßnahmen sind also noch keine hinreichenden Gründe für Allokationsineffizienzen, welche eine staatliche Regulierungspolitik rechtfertigen können.

1.3.3 Besonderheiten der getrennten Produktion von Basisgut und Sicherheitsmaßnahmen

Bisher wurde unterstellt, daß die Sicherheitsausstattungen gemeinsam mit dem risikobehafteten Gut hergestellt werden und die dadurch realisierten Economies of Scope potentiell zu Monopolen führen können oder es durch Produktdiversifikation aufgrund unterschiedlicher Qualitätspräferenzen zu monopolistischer Konkurrenz kommen kann. Aber auch die getrennte Produktion kann zu Allokationen führen, welche nicht paretoeffizient sind.

Kompatibilität zwischen Sicherheitsausstattung und Basisprodukt

Indem die Anbieter auf die Kompatibilität ihrer Produktkomponenten mit denen anderer Anbieter verzichten bzw. diese bewußt verhindern, werden die Nachfrager

---

[89] Wohlfahrtsverluste stellen sich erst dann ein, wenn ein Monopolist das mit verschiedenen Sicherheitsausstattungen ausgestattete Basisprodukt bereitstellt, weil dann die Preise aller Produkttypen höher liegen werden und der Gesamtoutput geringer sein wird. Vgl. dazu Hirshleifer & Glazer (1992), S.245f.

[90] Diese können u. a. von der oben dargestellten Kuppelproduktion verursacht werden.

[91] Vgl. dazu den richtungweisenden Beitrag von Dixit & Stiglitz (1977).

gezwungen, das komplette System von einem Hersteller zu beziehen.[92] So können durch die i. d. R. begrenzte technische Kompatibilität der Schadenpräventionsmaßnahmen mit dem entsprechenden risikobehafteten Produkt Ineffizienzen hervorgerufen werden.[93] Die meisten Nachfrager werden bezogen auf die gewünschte Qualität nicht ihre maximale Konsumentenrente realisieren, weil ihre Präferenzen von dem angebotenen Produktsystem abweichen, wenn zu dem betrachteten Basisprodukt nur ein kompatibles Sicherheitssystem auf dem Markt erhältlich ist.

Wie ändert sich nun die gesamtwirtschaftliche Wohlfahrt, wenn nun mehrere kompatible Sicherheitssysteme zur Verfügung stehen und die Produktvielfalt dadurch erhöht wird? Die Gesamtnachfrage wird steigen, da durch die gestiegene Kombinationsvielfalt den Konsumentenpräferenzen stärker entsprochen wird und damit die Zahlungsbereitschaft steigt. Jedoch wird sich der Preiswettbewerb entschärfen, weil eine Preissenkung einer Systemkomponente durch einen Anbieter nicht mehr - wie im Falle der Inkompatibilität - nur die Nachfrage nach seinem Produkt bzw. System steigt, sondern durch die Kompatibilität auch die Systeme aller anderen Anbieter billiger werden. Dies bedeutet, daß im Gegensatz zum Fall inkompatibler Systemkomponenten die Umsatzsteigerungen durch Preissenkungen nicht mehr alleine beim preissenkenden Anbieter anfallen, sondern auch bei allen anderen Anbieter von kompatiblen Systemkomponenten. Diese unvollkommene Internalisierung der Erträge wird zu einer Einschränkung von Preissenkungen führen. Der Effekt einer zunehmenden Produktkompatibilität auf die gesamtwirtschaftliche Wohlfahrt bleibt unbestimmt. Jedoch wird bei einer geringen Anzahl von existierenden kompatiblen Produkten durch die relativ starke Erhöhung der Produktvielfalt und der Internalisierung eines großen Anteils der Erträge einer Preissenkung der gesamtwirtschaftliche Nutzengewinn vermehrter Kombinationsmöglichkeiten größer sein als die anfallenden Nutzenverluste, so daß nur in diesem Fall eventuell ein staatlicher Eingriff gerechtfertigt werden kann.[94]

Bedeutende Wohlfahrtsverluste durch unzureichende Kompatibilität zwischen dem Basisprodukt und den Sicherheitsausstattungen anderer Anbieter drohen vor allem

---

[92] Dies wurde z. B. häufig in der Computerbranche beobachtet. Vgl. allgemein zur Kompatibilitätsthematik Tirole (1988), S. 335f.

[93] In der Fallstudie wird diese Problematik v. a. bei der Nachrüstung bestehender Kommunikationssysteme mit Mechanismen der Informationssicherheit diskutiert.

[94] Einhorn (1992) beweist, daß für ein Duopol die gleichen Wirkungen gelten. Kompatibilität führt tendenziell zu höheren Preisen, besonders für diejenigen Konsumenten, die ihre Komponenten von einem Anbieter bzw. ein komplettes System kaufen. Andererseits erweitern kompatible Komponenten die angebotene Produktvielfalt.

in einem Markt mit einer schwach ausgeprägten Produktvielfalt. In differenzierteren Märkten besteht diese Gefahr nicht mehr.

Kopplungsgeschäfte

Besteht technische Kompatibilität zwischen den Basisprodukten und den Sicherheitssystemen, können die Anbieter durch Kopplungsgeschäfte („bundling" oder „tie-in-sale") die Wahlmöglichkeiten der Nachfrager einschränken. Als Kopplungsgeschäft wird der Verkauf eines Bündels homogener[95] oder heterogener Güter bezeichnet. In diesem Kontext bedeutet letzterer Fall das gemeinsame Angebot von Basisprodukt und der dazugehörigen Sicherheitsausstattung, obwohl beide Produkte separat hergestellt werden. Das Basisprodukt kann also nicht ohne die Sicherheitsausstattung erworben werden.[96]

Falls nun ein Monopolist im Bereich des Basisgutes die Möglichkeit hat, die komplementären Güter den Verbrauchern gemeinsam zu verkaufen, wird er u. U. das Basisgut zum Grenzkostenniveau veräußern, aber die komplementären Sicherheitsmaßnahmen zu einem Preis über dem Grenzkostenniveau anbieten.[97] Dieser „tie-in-sale" verringert die Gesamtwohlfahrt, solange dieser Produzent Konsumenten mit unterschiedlichen Nachfrageintensitäten versorgt. Jedoch kann dies durch die im Vertrieb und Verkauf realisierten Skalenerträge begründet werden.[98] Ein Verbot des gemeinsamen Verkaufs würde dazu führen, daß zumindest die Sicherheitsmaßnahmen zum effizienten Grenzkostenniveau angeboten werden würden.[99] Zwar wird eine so geartete staatliche Regulierung den Monopolisten schädigen, aber die Konsumenten i. d. R. nicht begünstigen, weil u. U. nur noch die Nachfrager mit intensiven Präferenzen versorgt werden.[100]

---

[95] Wenn der Konsument dazu gezwungen wird, mehrere Einheiten des gleichen Gutes zu kaufen ist dies i. d. R. nicht wohlfahrtsoptimal, weil sein Handlungsspielraum eingeschränkt wird. Vgl. dazu Adams & Yellen (1976), S. 475ff.

[96] Untersuchungen von Kopplungsgeschäften bzgl. heterogener Güterbündel beziehen sich vor allem auf den gemeinsamen Verkauf von Hard- und Software in der Computerindustrie. Vgl. dazu Lunn (1990), S. 249-260, und Brennan & Kimmel (1986), S. 490-501. Indirekt ergeben sich Kopplungsgeschäfte auch durch die Inkompatibilität der Produktkomponenten verschiedener Hersteller.

[97] Vgl. dazu Tirole (1988), S. 147. Liebowitz (1983) argumentiert, daß Preisdifferenzierungsmotiven von „tie-in-sales" eher untergeordnete Bedeutung zukommt und die daraus resultierenden Effekte unbestimmt sind.

[98] Vgl. Tirole (1988), S. 159.

[99] Vgl. ebenda S. 147.

[100] Vgl. ebenda S. 148. Auch Adams & Yellen (1976) plädieren im Fall von „commodity bundling" (= Verkauf mehrerer gleicher Güter in einem Paket) und einer Monopolsituation dafür, das effizien-

Beim Bündeln von heterogenen Gütern, wie es im Fall eines Basisproduktes und separaten Sicherheitsausstattungen gegeben ist, besteht die Schwierigkeit darin, Annahmen über die Präferenzintensitäten für die verschiedenen Produkte machen zu müssen, so daß man sich in der Literatur nur auf konkrete Beispiele konzentriert und auf allgemein gültige Aussagen verzichtet hat.[101]

Kopplungsgeschäfte von komplementären Gütern können zwar durchaus Allokationsineffizienzen verursachen.[102] Aber bedeutende Wohlfahrtsverluste entstehen erst dadurch, wenn der Anbieter auf dem Markt eines Gutes eine Monopolstellung innehat. Deshalb bieten Kopplungsgeschäfte keine hinreichenden Gründe für eine staatliche Intervention in das Angebot von Sicherheitsmaßnahmen.

1.3.4 Informationsasymmetrien auf Versicherungsmärkten und ihre Rückwirkungen auf die Nachfrage nach Sicherheitsgütern

Da es sich bei der Versicherungsmöglichkeit um eine substitutive bzw. komplementäre Alternative[103] zur Absicherung bzw. Abwendung von Schadensfällen handelt, muß auch untersucht werden, welche Ineffizienzen auf den Versicherungsmärkten auftreten können. Denn dadurch können sich auf indirekten Kanälen volkswirtschaftlich unerwünschte Ergebnisse auf dem Markt für Schadenpräventionsgüter einstellen.[104] Deshalb werden die durch Informationsdefizite bzw. durch asymmetrische Informationsverteilung hervorgerufenen Erscheinungen wie Moral Hazard

---

tere Ziel der Monopolbeseitigung anzustreben anstatt das „bundling“ zu untersagen, welches u. U. Wohlfahrtsgewinne einbringen kann.

[101] Vgl. Tirole (1988), S. 160. In Lunn (1990) werden Kopplungsgeschäfte auch durch Risikoreduktion bei Einführung von innovativen Kapitalgütern begründet, und es kann nicht eindeutig gezeigt werden, daß solche Verträge wohlfahrtsmindernd sind. Sie können u. U. sogar zur schnelleren Verbreitung neuerer Technologien beitragen.

[102] Matutes & Regibeau (1992) zeigen, daß bei kompatiblen Komponenten in einem exzessiven Maße den Nachfragern Kopplungsgeschäfte angeboten werden. Besteht die Wahlmöglichkeit, Einzelkomponenten von den verschiedenen Herstellern zu erwerben oder das komplette System von einem Anbieter zu kaufen, dann werden zu intensive Standardisierungsbemühungen unternommen.

[103] Nach Ehrlich & Becker (1972), Chang & Ehrlich (1985) u. a. handelt es sich bei einer Versicherung um ein Substitut zu Self-insurance und um ein Komplement zu Self-protection.

[104] Es handelt sich hier um versicherungsangebotsinduzierte Effekte auf die Nachfrage nach Sicherheitsgütern, so daß sich auch eine Eingliederung in das folgende Kapitel über nachfragebedingte Allokationsineffizienzen rechtfertigen ließe. Denn die Bedingungen des Versicherungsangebotes wirken sowohl auf das Ausmaß als auch auf die Elastizität der Nachfrage nach Sicherheitsgütern.

und adverse Selektion in Versicherungsmärkten und ihre Rückwirkungen auf die Sicherheitsgüternachfrage analysiert.[105]

Die Versicherungsmärkte zeichnen sich durch zwei verschiedene Arten von Informationsasymmetrien aus.[106] Zum einen spricht man von Moral Hazard, wenn der Versicherungsnehmer aufgrund des erworbenen Versicherungsschutzes sein Verhalten bzgl. der ursprünglichen Schadenverhütungs- und Schadenverminderungsmaßnahmen verändert, wobei diese Verhaltensänderung vom Versicherer nicht beobachtet werden kann.[107] Zum anderen tritt das Phänomen der adversen Selektion[108] auf, wenn verschiedene Risikotypen mit unterschiedlich hohen Schadenswahrscheinlichkeiten vom Versicherer nicht identifiziert werden können, so daß eine differenzierte Prämiengestaltung nicht wirksam durchgesetzt werden kann und nicht alle Versicherungsnachfrager den von ihnen bei vollkommener Transparenz gewünschten Vollversicherungsschutz erhalten können.

Moral Hazard

Da es sich bei einer Versicherung um ein Substitut zu Schadenbegrenzungsgütern handelt, wird das Individuum eine Kombination von Marktversicherung und Self-insurance wählen, die zu einem Ausgleich der Grenzproduktivitäten beider Strategien führt.[109] Wie bereits gezeigt, wird es in einem Szenario vollkommener Information bei aktuarisch fairen Prämien eine Vollversicherung wählen. Neben der Versicherung gegen den Schadensfall bleibt dem Individuum dennoch die zusätzliche Möglichkeit, Sicherheitsvorkehrungen zu treffen, welche die Prämienhöhe zu reduzieren vermögen. Falls der Versicherer das vom Versicherten unternommene Präventionsniveau beobachten kann, kommt es zum First-Best-Optimum, weil sich die Prämiensätze am "level of care" bzw. am unterstellten Erwartungsschaden aus-

---

[105] Vgl. zu den Allokationsineffizienzen auf Versicherungsmärkten u. a. Strassl (1988).

[106] Vgl. Schulenburg (1992), S. 404, oder Pauly (1974).

[107] Im Kontext von Abschnitt 1.2.3.4 bedeutet dies, daß die wahren Werte von Schadeneintrittswahrscheinlichkeit p und Schadenhöhe L über denen liegen, welche die Versicherung für die Berechnung ihrer Prämiensätze zugrunde legt, weil der Versicherte seine Aufwendungen für die Schadenpräventionsmaßnahmen s nach Abschluß der Versicherung ändert. Vgl. dazu allgemein u. a. Asch (1988), S. 57, und Pauly (1974), S. 48f.

[108] Bezogen auf den Abschnitt 1.2.3.4 besagt dies, daß der Versicherer nicht in der Lage ist, die Versicherten nach ihren als exogen angenommenen Schadeneintrittswahrscheinlichkeiten p zu differenzieren. Vgl. dazu u. a. Asch (1988), S. 58, Pauly (1974), S. 54f und den ausführlichen Überblick von Richter (1995).

[109] Vgl. dazu Ehrlich & Becker (1972), S. 636. Beim Ausgleich der Grenzproduktivitäten von kombinierten Schadenverhütungsmaßnahmen und einer Marktversicherung müssen zusätzlich komplementäre Beziehungen der beiden Strategien beachtet werden, welche aber aus Gründen der Anschaulichkeit nicht weiter untersucht werden.

richten werden.[110] Die Existenz einer Versicherung führt also zu einem wohlfahrtssteigernden Rückgang der individuellen Nachfrage nach Sicherheitsgütern, weil von diesen nur noch soviel nachgefragt werden, bis ihre Grenzproduktivität die einer Marktversicherung erreicht.[111]

Ist dagegen dem Versicherer die Beobachtung der Schadenverhütungsmaßnahmen nicht möglich, ist auch die gesamtwirtschaftliche Nachfrage nach Schadenprävention nicht mehr effizient bzw. die First-Best-Lösung. Bei der Möglichkeit zur Vollversicherung hat der Versicherte überhaupt keinen Anreiz mehr, Schadenverhütung durchzuführen, da er nun indifferent zwischen Schadens- und Nichtschadensfall wird. Den positiven Effekt, den seine Vorsorgemaßnahmen auf die Versicherungsprämienhöhe hat, berücksichtigt er in seinem Nutzenmaxmierungskalkül nicht mehr. Die Prämie wird nämlich gemäß seiner ex ante festgestellten Schadenswahrscheinlichkeit und -höhe ohne Beachtung seiner aktuellen Sicherheitsanstrengungen festgelegt. Dies bedeutet aber Moral Hazard, d. h. die ursprünglich unternommenen Schadenpräventionsmaßnahmen werden auf Null gesenkt, da eine vollständige Schadenskompensation durch die Versicherung gegeben ist. Aufgrund des Informationsdefizits der Versicherung bzgl. der wahren nach Vertragsabschluß sich einstellenden Schadeneintrittswahrscheinlichkeit und potentiellen Schadenhöhe werden ihr Verluste entstehen, weil der erwartete Schaden höher ausfallen wird als die Summe der eingezahlten Prämien.[112] Jedoch wird die Versicherung auf den Informationsnachteil so reagieren, indem sie vom gewählten Deckungsgrad auf die unternommenen Präventionsmaßnahmen bzw. auf die Schadeneintrittswahrscheinlichkeit schließt und den Aufschlag mu progressiv mit dem Deckungsgrad d ansteigen läßt.[113] Die Folge einer solchen Strategie ist, daß sorgfältige und vorsichtige

---

[110] Die Schadenpräventionsmaßnahmen reduzieren also nicht nur den Erwartungsschaden, sondern führen bei der Beobachtbarkeit durch den Versicherer dazu, daß dessen geforderte Prämienhöhe nach unten korrigiert wird. Vgl. dazu auch die Darstellung in Strassl (1988), S. 42f und 54ff.

[111] Vgl. dazu auch Chang & Becker (1985), S. 583, welche die Interdependenzen zwischen Self-protection und Selbstversicherung bei Existenz und Nichtexistenz einer Marktversicherung untersuchen.

[112] Neben dem Verlust für den Versicherer entsteht auch ein gesamtwirtschaftlicher Wohlfahrtsverlust, weil Schadenvermeidungsaktivitäten, welche höhere Grenznutzen einbringen als sie Grenzkosten verursachen, nicht unternommen werden. Vgl. zu den positiven externen Effekten von Schadenspräventionsmaßnahmen Abschnitt 1.4.5.

[113] Diese Strategie ist aber nur dann erfolgreich, wenn die verschiedenen Versicherungsanbieter kooperieren, indem sie verhindern, daß ein Versicherungsnehmer mehrere Bruchteilversicherungen bei verschiedenen Anbietern abschließen kann und so eine Vollversicherung zu fairen Prämien erhält. Den gleichen Effekt erhält man, wenn eine Monopolversicherung unterstellt wird.

Individuen nur noch eine Bruchteilversicherung[114] wählen und außerdem positive Schadenverhütungsmaßnahmen unternehmen werden.[115] Nur fahrlässige Wirtschaftssubjekte mit sehr hohen Risiken bzw. Schadenswahrscheinlichkeiten werden eine Vollversicherung wählen, welche sie Prämienzahlungen kosten wird, die ihre maximale Zahlungsbereitschaft nahezu ausschöpfen. Gesamtwirtschaftlich bleibt das bei vollkommener Transparenz sich einstellende Paretooptimum zwar unerreicht, jedoch resultiert aus der deckungsgradabhängigen Prämiensetzung eine Paretoverbesserung gegenüber der deckungsgradunabhängigen Prämiensatzstrategie und damit auch eine stärkere Nachfrage nach Sicherheitsvorkehrungen.[116]

Bei vollkommener Informiertheit der Versicherer führt die Existenz einer Versicherung zu einer wohlfahrtserhöhenden Substitution eines Teils der Sicherheitsmaßnahmen. Die Möglichkeit von Moral Hazard vermindert dagegen die Nachfrage für Schadenspräventionen vollständig, wenn die Versicherung keinerlei Anhaltspunkte bzgl. der individuellen Vorsorge hat. Schließt sie dagegen indirekt vom gewählten Deckungsgrad auf die unternommenen Schutzmaßnahmen und macht sie den Aufschlag auf die faire Prämie progressiv vom Deckungsgrad abhängig, wird sich die Nachfrage weniger reduzieren, da die meisten Individuen keine Vollversicherung mehr wählen und statt dessen einen positiven Betrag für Sicherheitsmaßnahmen ausgeben werden.

---

[114] Eine weitere Strategie zur Vermeidung von Moral Hazard sind neben der Bruchteilversicherung als relativer Selbstbeteiligung auch die Festlegung eines Selbstbehaltes bzw. einer absoluten Selbstbeteiligung.

[115] Können die Wirtschaftssubjekte nur noch eine Bruchteilversicherung abschließen, sind zwei Fälle zu unterschieden. Falls der Versicherer die Anstrengungen der Versicherten nicht beobachten kann, wird in deren Nachfrage nach Sicherheitsgütern als Determinante nur noch der Rest des Schadens einfließen, der nicht von der Versicherung entschädigt wird, so daß ein suboptimales Präventionsniveau gewählt wird. Zu umfangreiche Sicherheitsvorkehrungen werden getroffen, wenn diese zusätzlich zu einer Reduktion der zu zahlenden Versicherungsprämie führen, was aber hinsichtlich der unterstellten Informationsprobleme der Versicherer unrealistisch ist.

[116] Vgl. dazu auch Eisen (1990), S. 125-128. Bei der Möglichkeit zur Vollversicherung trotz Moral Hazard müßten die Kosten von Sicherheitsmaßnahmen wegen ihrer positiven externen Effekte auf den Versicherer durch Subventionen theoretisch auf null gesenkt werden, und dann ist immer noch nicht gewährt, daß die Versicherungsnehmer die gesamtwirtschaftlich optimale Vorsorge treffen. Nur wenn die Versicherung nicht alle Schäden kompensieren kann, haben Sicherheitsmaßnahmen einen positiven Grenznutzen und Subventionen eine positive Wirkung auf die unternommene Vorsorge. Vgl. zu dieser Thematik Strassl (1988), S. 100-113. Da i. d. R. keine Vollversicherungsmöglichkeit besteht, wird auch immer Vorsorge getroffen werden. Deshalb können versicherungsmarktendogene Fehlallokationen eine staatliche Intervention auf dem Markt für Sicherheitsvorkehrungen nicht generell rechtfertigen und werden hier nicht weiter diskutiert.

Adverse Selektion

Bisher wurden identische Individuen angenommen, so daß von einem repräsentativen Versicherungsnachfrager bzw. Sicherheitsgüternachfrager ausgegangen werden konnte. Diese Vereinfachung wird nun aufgegeben und durch die Annahme der Existenz von zwei Risikotypen mit hoher bzw. geringer, exogen gegebener Schadenswahrscheinlichkeit ersetzt.[117] Kann der Versicherer die unterschiedlichen Risikotypen identifizieren, werden die Prämiensätze nach der Schadeneintrittswahrscheinlichkeit differenziert, so daß die Individuen jeweils eine Vollversicherung abschließen werden.[118]

Bei Unkenntnis der Risikotypen ist die Versicherung neben der Gefahr des Moral Hazard auch dem Phänomen der adversen Selektion ausgesetzt.[119] Dies bedeutet, daß bei der Existenz von Individuen mit unterschiedlichen, von den Versicherern nicht identifizierbaren Schadeneintrittswahrscheinlichkeiten die Gefahr der negativen Auslese besteht, weil die guten Risiken keine Versicherung mehr nachfragen werden. Denn die eigentlich für die guten Risiken konzipierten Verträge, welche auf der Basis von geringen Schadeneintrittswahrscheinlichkeiten kalkuliert sind, werden auch von den schlechten Risiken gekauft werden, so daß die nach der erwarteten Schadeneintrittswahrscheinlichkeit differenzierten Prämiensätze unwirksam sein werden. Dieses Verhalten führt jedoch zu negativen Gewinnen für die Versicherungsgesellschaft. Da langfristig betrachtet negative Gewinne für die Versicherung kein Gleichgewicht darstellen, wird das bei Kenntnis der Risikotypen differenzierte Kontraktangebot aufgegeben und nur zu hohen Prämiensätzen, welche sich nach den schlechten Risiken richten, eine Vollversicherung angeboten.[120] Dieses Angebot ist jedoch für die guten Risiken nicht wohlfahrtssteigernd.[121] Deshalb werden sie sich auf Teilversicherungsverträge beschränken, welche zu günsti-

---

117 Diese Annahme läßt sich dadurch begründen, daß die Individuen zwar Einfluß auf ihr Risiko nehmen können, dies aber grundsätzlich nichts an der Einteilung in gute und schlechte Risikotypen ändert. Strenggenommen können sich die Risikotypen auch durch ihre potentiellen Schadenausmaße unterscheiden. Jedoch sind die Versicherungsverträge i. d. R. so ausgestaltet, daß bzgl. der Kompensation ex ante zumindest Höchstgrenzen festgelegt werden und dadurch das quantitative Risiko seitens der Versicherer begrenzt wird.

118 Vgl. dazu u. a. Strassl (1988), S. 128ff.

119 Vgl. Strassl (1988), S. 138ff.

120 Vgl. auch dazu Tirole (1988), S. 150: „A risk-neutral monopoly insurance company optimally discriminates between the consumers by giving full insurance (the socially optimal policy) to high-risk consumers and suboptimal insurance to low risk consumers."

121 Die maximale Zahlungsbereitschaft ist die Summe aus Erwartungsschaden und individuellem Risikopreis. Vgl. dazu Abschnitt 1.2.3.4. Deshalb sind u. U. sehr risikoaverse Individuen mittleren Risikos auch bereit, Vollversicherungen zu unfairen Prämien abzuschließen, wenn keine günstigen Substitutionsmöglichkeiten existieren.

geren Prämiensätzen zu erwerben sind.[122] Unter gewissen Umständen kommt es jedoch zu einer vollständigen Verdrängung der guten Risiken vom Versicherungsmarkt, so daß dann nur noch für die schlechten Risiken konzipierte Vollversicherungsverträge angeboten werden.

Es wurde in diesem Abschnitt von zwei Risikotypen mit exogen gegebenen Schadeneintrittswahrscheinlichkeiten ausgegangen. Betrachtet man die Veränderung der aggregierten Nachfrage nach Sicherheitsgütern unter der Annahme vollständiger adverser Selektion auf dem Versicherungsmarkt im Vergleich zu einem perfekten Versicherungsmarkt, wo die Identität der Risikotypen bestimmbar ist, können folgende Tendenzen festgestellt werden.

Unter der Annahme vollständiger Informiertheit der Versicherung über das Verhalten der Individuen führt die Versicherungsmöglichkeit zunächst zu einem wohlfahrtssteigernden Nachfragerückgang nach Schadenpräventionsgütern, weil es zu einer Teilsubstitution durch die billigere Versicherungslösung kommt. Bei adverser Selektion werden die schlechten Risiken eine Vollversicherung wählen, und ihre Nachfrage nach Schadensbegrenzungsgütern wird sich unter Vernachlässigung von Moral Hazard nicht verändern. Im Gegensatz dazu werden sich die guten Risiken im Fall von adverser Selektion nur noch zum Teil oder überhaupt nicht mehr versichern, so daß sie den preisinduzierten Nachfragerückgang nach Versicherungsschutz durch eine erhöhte Nutzung von Präventionsmaßnahmen ausgleichen werden. Deshalb steigt ihre Nachfrage nach Schadenspräventionen mit zunehmender Informationsasymmetrie an, weil sie nicht mehr die optimale Vollversicherung nachfragen werden. Falls sich im Fall vollkommener Transparenz die gesamtwirtschaftlich effiziente Sicherheitsgüternachfrage einstellt, dann ergibt sich im Fall von adverser Selektion auf dem Versicherungsmarkt auch auf dem Schadenspräventionsgütermarkt ein Wohlfahrtsverlust, weil die relativ günstigere Versicherungsmöglichkeit durch die guten Risiken zu wenig genutzt werden kann.

Unterstellt man gleichzeitig durch asymmetrische Informationsverteilung induzierten Moral Hazard und adverse Selektion auf den Versicherungsmärkten können für die Nachfrage nach Schadensprävention zusammenfassend folgende Schlüsse gezogen werden:

[122] Vgl. Strassl (1988), S. 151. Bei adverser Selektion können sich je nach Verhalten der Angebotsseite weitere Gleichgewichte einstellen. Vgl. Richter (1995), Kap. 3 und 4.

Erstens führt die Möglichkeit von Moral Hazard zunächst einmal zum vollständigen Rückgang der Nachfrage für Schadenspräventionen, wenn die Versicherung keinerlei Anhaltspunkte über die individuellen Vorsorgebemühungen hat. Schließt sie dagegen indirekt vom gewählten Deckungsgrad auf die unternommenen Schutzmaßnahmen und macht sie den Aufschlag auf die faire Prämie progressiv vom Deckungsgrad abhängig, wird sich die Nachfrage weniger reduzieren, da die meisten Individuen keine Vollversicherung mehr wählen werden. Zweitens bewirkt die Verdrängung der guten Risiken aus dem Versicherungsmarkt durch adverse Selektion, daß diese ersatzweise verstärkt Schadenpräventionsmaßnahmen nachfragen werden, obwohl es volkswirtschaftlich betrachtet günstiger ist, die Vollversicherungslösung zu fairen Prämien zu wählen. Somit stellen sich durch die Informationsasymmetrien auf den Versicherungsmärkten tendenziell zwei konterkarierende Effekte auf die Nachfrage nach Sicherheitsgüter ein, so daß keine eindeutige Gesamtwirkung zu bestimmen ist. Jedoch wird sich die Elastizität der Nachfrage nach Sicherheitsmaßnahmen um so stärker verringern, desto größer die Informationsasymmetrien auf dem Versicherungsmarkt sein werden, weil in dem Fall immer weniger Individuen den Preis der von ihnen gewünschten Vollversicherung zu zahlen bereit sind. Unterstellt man gar Nichtversicherbarkeit durch einen privaten Versicherungsanbieter, dann entfällt für alle Individuen die Marktversicherung als Substitut zu den Sicherheitsvorkehrungen und die in den beiden vorangegangenen Abschnitten dargestellten Quellen von Ineffizienzen können u. U. stärkere Wohlfahrtsverluste verursachen.

1.3.5. Fazit

Es existieren zwar eine Reihe von Besonderheiten bzgl. des Angebotes an Sicherheitsmaßnahmen, welche Allokationsineffizienzen auslösen können. Jedoch können darüber keine allgemeine Aussagen getroffen werden, weil produktions- und absatztechnische Details entscheidend sind. Die potentiell entstehenden Wohlfahrtsverluste sind aber nur dann bedeutend, wenn die Anbieter der Basisprodukte oder auch der Sicherheitsmaßnahmen selbst Monopolstellungen innehaben. Deshalb werden auch keine speziellen staatlichen Instrumente, wie sie bezüglich nachfrageseitig bedingter Allokationsineffizienzen in Kapitel 1.5 dargestellt werden, disku-

tiert.[123] Statt dessen ist zu betonen, daß sich staatliche Interventionen darauf beschränken sollten, die Offenheit der Märkte für potentielle Konkurrenz zu gewährleisten.[124]

Hinsichtlich der durch Informationsasymmetrien begründeten Ineffizienzen des Versicherungsangebotes, welche die Elastizität der Nachfrage nach Sicherheitsgütern reduziert, wird darauf hingewiesen, daß eine staatliche Regulierung der Versicherungsmärkte[125] besonders dann nachhaltig auf die Nachfrage nach Sicherheitsvorkehrungen wirkt, wenn das Versicherungsangebot für einen Teil oder gar für alle Wirtschaftssubjekte suboptimal ist oder überhaupt nicht existiert. Können alle Wirtschaftssubjekte zumindest Bruchteilversicherungen erhalten, dann wird der Effekt auf die Nachfrage nach Sicherheitsvorkehrungen nicht so stark sein, daß dadurch ein staatlicher Eingriff in die Versicherungsmärkte gerechtfertigt werden kann.

---

[123] Auch in der Fallstudie wird hinsichtlich des Marktes für Kommunikationsnetze und -dienste Wettbewerb unterstellt, damit sich in der Analyse auf nachfragebedingte Ursachen für Fehlallokationen im Bereich der Informationssicherheit beschränkt werden kann.

[124] Vgl. dazu u.a. Fritsch, Wein und Ewers (1993), S. 141f. Falls es sich bei der Produktion des betreffenden Konsumgutes um ein natürliches Monopol handelt, dann sollte sich sein Aktivitätsbereich nicht auf vor- oder nachgelagerte Märkte beziehen, weil es durch Dumping-Strategien, finanziert durch die Monopolgewinne, auch dort eine marktbeherrschende Stellung einnehmen kann. Die aktuelle Situation auf den deutschen Märkten für Wach- und Sicherheitsunternehmen zeichnet sich inzwischen durch einen harten Preiswettbewerb aus, so daß kein staatlicher Eingriff legitimiert werden kann. Vgl. o. V. (1995b).

[125] Auf die staatliche Regulierungsmöglichkeiten bzgl. des Versicherungsangebotes wird lediglich in Abschnitt 2.5.5 der Fallstudie eingegangen, weil in diesem Fall ein privates Versicherungsangebot unvollständig bzw. nichtexistent ist. Vgl. allgemein zu staatlicher Regulierung bei Moral Hazard Strassl (1988), S. 91-100, und bei adverser Selektion ebenda, S. 153-158 u. S.177-190.

1.4 Ursachen nachfragebedingter Allokationsineffizienzen auf Märkten für Sicherheitsgüter und -maßnahmen

1.4.1 Vorbemerkungen

Nachdem im vorangegangenen Kapitel die Besonderheiten des Angebotes an Sicherheitsvorkehrungen, die Informationsasymmetrien auf den Versicherungsmärkten und die daraus resultierenden potentiellen Ineffizienzen dargestellt wurden, besteht die Absicht dieses Kapitels darin, Ursachen von Allokationsineffizienzen bzw. Marktversagen, welche von der Nachfrageseite herrühren, zu analysieren.[126] Dabei wird sich vor allem auf die Funktion s* von Gleichung (19) und ihre Determinanten bezogen.

Zunächst wird untersucht, ob die beiden charakteristischen und nicht immer exakt voneinander trennbaren Gründe für die Bereitstellung sogenannter meritorischer Güter, nämlich Irrationalität und unvollständige bzw. asymmetrische Information der Wirtschaftssubjekte[127], auch bei Sicherheitsmaßnahmen zutreffen. Deshalb wird zuerst auf Entscheidungsanomalien eingegangen, welche bei Unsicherheit zu beobachten sind und mit erwartungsnutzenmaximierendem Verhalten nicht im Einklang stehen und deshalb als irrational gelten.[128] Danach werden Informationsdefizite der Nachfrager hinsichtlich bestimmter Nachfragedeterminanten aufgegriffen, welche auch zu den i. d. R. Versicherungsmärkten zugeordneten Erscheinungen Moral Hazard und adverser Selektion führen können. Obwohl durchaus Marktanreize zum Abbau von Informationsasymmetrien existieren, verhindern bestimmte Eigenschaften, daß es zu vollständiger Markttransparenz kommt. Dieses wird im dritten Abschnitt problematisiert. Daran anschließend wird die im Kontext von Sicherheitsmaßnahmen wichtige Rolle von externen Effekten untersucht. Das Kapitel

---

126 Vgl. allgemein zu den mikroökonomischen Grundlagen verschiedener Marktversagensursachen Fritsch, Wein und Ewers (1993). Spezifischer bzgl. der Marktversagensgründe von Produktsicherheit ist die Übersicht in Oi (1973), S. 3-28. Der Beitrag von Panzar & Savage (1989), S. 35-40, bezieht sich auf die Problematik im Bereich der Transportsicherheit.

127 Vgl. dazu Head (1966), S. 4ff, und Head (1969), S. 215ff.

128 Es existieren zwei Strategien, um mit diesen Irrationalitäten umzugehen. Vgl. dazu Eichenberger & Frey (1990), S. 272-274. Zum einen kann eine Abwehrhaltung eingenommen und die traditionelle Erwartungsnutzenhypothese verteidigt werden, indem von vernachlässigbaren Ausnahmen und lernfähigen Individuen ausgegangen wird. Zum anderen kann der Erwartungsnutzenansatz modifiziert werden, um auch solche nach dem traditionellen Ansatz irrationalen Verhaltensweisen erklären zu können. Vgl. dazu Asch (1988), S. 40-43, und S. 80ff und die dort angegebenen Literaturhinweise.

schließt mit einer Übersicht über die Gründe von Allokationsineffizienzen bzw. Marktversagen.

1.4.2 Irrationales Nachfragerverhalten

Die traditionelle Entscheidungstheorie unterstellt normalerweise rational handelnde Wirtschaftssubjekte. In diesem Abschnitt wird diese strenge Annahme aufgehoben, und es wird darauf eingegangen, inwieweit Entscheidungen unter Unsicherheit irrational ausfallen können, welchen Einfluß dies auf die Nachfrage nach Sicherheitsgütern und -maßnahmen hat und warum es deshalb zu Fehlallokationen kommen kann.[129]

Der Referenzrahmen der Analyse ist ein Verhalten nach dem Erwartungsnutzenkonzept, welches als Grundlage der theoretischen Ableitung der Nachfrage nach Sicherheitsmaßnahmen gedient hat. Dem Individuum seien auch alle für die Erwartungsnutzenmaximierung notwendigen Informationen bekannt. Das ineffiziente Verhalten begründet sich also nicht durch eine unzureichende oder asymmetrische Informationslage, sondern durch das irrationale Verhalten unter Unsicherheit aufgrund inadäquater Informationsverarbeitung und paradoxer Entscheidungen.

Die folgenden von der Rationalität der Erwartungsnutzenmaximierung abweichenden Verhaltensweisen werden bei Entscheidungen unter Unsicherheit häufig beobachtet.[130]

Trotz der Verfügbarkeit aller für eine rationale Entscheidung notwendigen Informationen machen die Individuen Fehler bei der Informationsverarbeitung, indem selektiv nur bestimmte objektive Informationen berücksichtigt werden.[131] Augenfällige Merkmale werden überbewertet, während Grundwahrscheinlichkeiten vernachlässigt werden.[132] Außerdem spielen wenige einprägsame und leicht zu be-

---

[129] Vgl. allgemein zur Nichtrationalität den Überblick von Fritsch, Wein und Ewers (1993), S. 247-251, und speziell zu Entscheidungsanomalien unter Unsicherheit Eichenberger & Frey (1990), Hirshleifer & Riley (1992), S. 33-39, und den gelungenen Übersichtsaufsatz von Machina (1987).

[130] Vgl. dazu den Überblick in Frey & Eichenberger (1989), S. 82-85, und die ausführliche Darstellung von Kahneman, Slovic und Tversky (1991).

[131] Vgl. zur selektiven Informationsverarbeitung Asch (1988), S. 74f.

[132] Dies bedeutet, daß allgemeine Angaben über das grundsätzliche Risiko einer Aktivität oder Gutes bei der Einschätzung nicht mehr berücksichtigt und durch wenig repräsentative Informationen verzerrt werden. Vgl. dazu Kahneman & Tversky (1991), S. 49-57. So wird das Risiko des Flugverkehrs bedingt durch katastrophale Einzelereignisse tendenziell überschätzt.

schaffende Hinweise bei der Entscheidungsfindung eine über Gebühr große Rolle, während die Gesamtheit vieler Detailinformationen oft unberücksichtigt bleibt.[133] So werden die relativ geringen Wahrscheinlichkeiten spektakulärer Schadensfälle stärker in die Entscheidung über die Ergreifung von Sicherheitsmaßnahmen einfließen als die Häufigkeit des Auftretens von alltäglichen Defekten. Die verzerrte Selektion von Informationen über Schadenswahrscheinlichkeiten und Schadenhöhen führt dazu, daß die Individuen suboptimale Entscheidungen bzgl. ihrer Schadenpräventionsmaßnahmen treffen werden.[134]

Neben dem mit der Erwartungsnutzenmaximierungsregel unvereinbaren Verhalten im Falle von Lotterien mit kleinen Gewinnwahrscheinlichkeiten, welches für diesen Kontext nicht von Bedeutung ist, kommt es häufig zu einer Überbewertung sicherer Gewinne relativ zu sehr hohen Gewinnwahrscheinlichkeiten.[135] Dies bedeutet für das Verhalten von Individuen bzgl. der zu ergreifenden Schadenpräventionsmaßnahmen, daß sie im Zweifel trotz eines übermäßig hohen Preises i. d. R. die 100%-sichere Alternative einer nur marginal weniger sicheren Ausgestaltung vorziehen, wobei dieses Verhalten nicht mehr nur durch sehr starke Risikoaversion erklärt werden kann.[136]

Abgesehen von den aufgezeigten Anomalien kommt noch hinzu, daß die Individuen bei der Bewertung von Gewinnen und Verlusten gewöhnlich vom status quo als Referenzpunkt ausgehen und dabei den Verlusten ein höheres Gewicht beimessen als den Gewinnen. Außerdem verhalten sie sich bzgl. verschiedener Verlustmöglichkeiten bei sehr kleinen Wahrscheinlichkeiten risikoavers, während sie andererseits gerne bereit sind, die sicheren Ausgaben für Schadensprävention zugunsten von geringeren Aufwendungen mit höheren erwarteten Verlusten einzutauschen. Dies führt dazu, daß die Wirtschaftssubjekte geneigt sind, nur suboptimale Scha-

---

133 Vgl. dazu u. a. Tversky & Kahneman (1991), S. 163-178.

134 Unterstellt man ein Szenario multipler Risiken, dann ist der oben dargestellte Effekt ambivalent, weil es zum einen zu einer Überschätzung geringer und zum anderen zu einer Unterschätzung hoher Schadenswahrscheinlichkeiten kommt, so daß auch nicht bestimmt werden kann, ob die nachgefragte Menge an Sicherheitsvorkehrungen zu hoch oder zu gering ausfällt.

135 Vgl. zum sogenannten "certainty effect" Asch (1988), S. 70f.

136 Die Ineffizienz eines solchen Verhaltens besteht darin, daß zu umfangreiche Sicherheitsvorkehrungen getroffen werden und damit der in diesem Fall sehr geringe Grenznutzen der zuletzt eingesetzten Einheit s kleiner ist als die mit ihrer Anschaffung anfallenden Grenzkosten.

denspräventionsmaßnahmen zu ergreifen und damit ein höheres Verlustrisiko bei geringeren Schadenvermeidungsaufwendungen eingehen.[137]

Ferner belegen empirische Untersuchungen, daß die Individuen häufig ihr persönliches Risiko unterschätzen, weil sie glauben, dieses unter Kontrolle zu haben.[138] So halten sich die meisten Autofahrer für überdurchschnittlich qualifizierte Fahrer. Die Nachfrage nach Schadenpräventionsmaßnahmen wird deshalb zu gering ausfallen, und es wird zu wenig Vorsorge betrieben.

Schließlich ist für das Verhalten des Individuums bedeutsam, in welcher Art es mit der Entscheidungssituation konfrontiert wird. So wird der Umfang der gewählten Schadenprävention auch davon abhängen, ob bei der Präsentation der Risikosituation der Grad der gewährten Sicherheit (1-p) oder die verbleibenden Schadenswahrscheinlichkeiten p zur Charakterisierung herangezogen werden. Hinsichtlich dieses Phänomens lassen sich jedoch keine eindeutigen Wirkungen auf das gewählte Schadenpräventionsniveau bestimmen.

Die dargestellten Anomalien zeigen auf, daß von den Individuen bei Entscheidungen unter Unsicherheit das nach der Erwartungsnutzentheorie abgeleitete optimale Niveau an Sicherheitsvorkehrungen nicht immer realisiert wird. Um diese Erscheinungen erklären zu können, wurden deshalb Modifikationen des Erwartungsnutzenansatzes entwickelt.[139] Aus Gründen der Operationalisierbarkeit wird in der weiteren Untersuchung die Erwartungsnutzenmaximierung jedoch als Referenzhandlungsweise beibehalten, jegliches Abweichen davon als irrational bezeichnet und als Ursache für allokative Ineffizienz angesehen.

---

137 Dies bedeutet, daß trotz Risikoaversion die Neigung besteht, ein billiges Sicherheitssystem mit geringerem Schutzwirkungen einem teureren, aber sichereren vorzuziehen. Ein solches Verhalten ist deshalb ineffizient, weil nicht bis zu dem Ausmaß Sicherheitsmaßnahmen ergriffen werden, welches einen Ausgleich von Grenznutzen und Grenzkosten herstellt, und damit mögliche Wohlfahrtsgewinne nicht realisiert werden.

138 Hier handelt es sich um eine Unterschätzung der Schadeneintrittswahrscheinlichkeit p bzw. um eine Überschätzung der Möglichkeiten, durch eigenes sorgfältiges Verhalten p vermindern bzw. die Effienz der Sicherheitsvorkehrungen steigern zu können. Vgl. zu weiteren Beispielen, welche von der Unterbewertung des individuellen Risikos zeugen, Asch (1988), S. 76-79, und die dort angegebenen Quellen.

139 Machina (1987), zeigt auf, daß nur einige der aufgeführten Verhaltensweisen durch die Aufgabe der strengen Annahme der Linearität der Neuman-Morgenstern-Funktion in ein erweitertes Erwartungsnutzenverständnis integriert werden können, aber ein Theorierahmen, der alle Anomalien vereinigt, noch nicht entwickelt werden konnte, so daß dadurch ein Festhalten an der Erwartungsnutzenhypothese gerechtfertigt werden kann.

Inwieweit und in welche Richtung die optimale Nachfrage nach Schadenpräventionsgüter durch die angeführten Verhaltensweisen verändert wird, läßt sich aufgrund der zum Teil entgegengesetzten Wirkungen nicht genau bestimmen. Aber abgesehen vom "certainty effect" neigen die Individuen dazu, zum einen ihr persönliches Verlustrisiko zu unterschätzen und zum anderen gerade bei Verlustrisiken eher die "riskantere" Alternative zu wählen. Sie scheuen sich also davor, Ausgaben für Sicherheitsmaßnahmen zu ergreifen, und sind statt dessen bereit, Verlustrisiken mit einer höheren Streuung ihrer Vermögenssituation einzugehen. Daraus läßt sich für die Nachfrage nach Schadenpräventionsgüter ableiten, daß diese tendenziell zu gering ausfallen wird.

Gerade meritorische[140] bzw. paternalistische[141] Rechtfertigungen von Sicherheitsstandards fußen darauf, daß die Individuen weniger Sicherheit nachfragen als der Staat für wünschenswert hält.[142] Besonders paternalistische Eingriffe des Staates in die Konsumentensouveränität werden allgemein und unspezifiziert damit begründet, daß die Betroffenen solche Vorgaben längerfristig betrachtet für erstrebenswert halten, weil damit ihre Handlungs- und Leistungskompetenz und so auch ihre Existenz gesichert wird.[143]

In der Realität verbergen sich paternalistische Argumentationselemente oft hinter den noch folgenden Informationsasymmetrieproblemen. Jedoch ist es nicht möglich, zu quantifizieren, zu welchen Teilen sicherheitsregulierende Interventionen jeweils den angesprochenen Marktversagensgründen oder paternalistischen Intentionen zugeordnet werden können. Deshalb und aufgrund der in der Realität vielfältig auftretenden Externalitäten von Sicherheitsmaßnahmen[144], welche nach der

---

140 In diesem Fall wird Meritorik ausschließlich durch die Irrationalität der Wirtschaftssubjekte legitimiert.

141 Paternalismus als allgemeinerer Begriff wird als wohlwollende Verhaltensmaßregelung für ein Individuum verstanden, welches diese Auferlegung nicht wünscht und welches durch seine Verhaltensänderung bei Dritten keine positiven externen Effekte auslöst. Übersetzung des Verfassers nach Asch (1988), S. 82: "the benevolent imposition on a person of a course of conduct where (1) the person does not desire the imposition and (2) the person's conduct has no important third-party (external) effects." Vgl. eine ähnliche Definition in VanDeVeer (1986), S. 22.

142 Vgl. dazu Gruenspecht & Lavé (1989), S. 1531f.

143 Vgl. dazu Priddat (1992), S. 251-256. Es können aber in jedem Fall zwei wesentliche Kritikpunkte an meritorischer Intervention bzgl. der Produktsicherheit konstatiert werden. Die durch paternalistische Handlungsweisen zu Begünstigenden werden in ihrer Würde und ihrer Konsumentenfreiheit beschnitten, was ihnen i. d. R. einen Wohlfahrtsverlust verursacht. Darüber hinaus entstehen dem Staat durch den regulierenden Eingriff hohe Kosten, da die Zielgruppe i. d. R. nicht exakt bestimmt werden kann und deshalb die ganze Bevölkerung in ihrem Verhalten begrenzt werden muß. Vgl. dazu Asch (1988), S. 82.

144 Vgl. dazu Abschnitt 1.4.5.

obigen Definition keine Rechtfertigung für paternalistische Interventionen darstellen, bleibt der paternalistische Einfluß in der staatlichen Regulierung von Sicherheitsvorschriften unklar und wird deshalb in der weiteren Analyse - besonders der verfügbaren wirtschaftspolitischen Instrumente - nicht mehr berücksichtigt, sondern es wird entweder konkret mit irrationalem Verhalten oder, wie unmittelbar folgend, mit Informationsasymmetrien argumentiert.

1.4.3 Informationsasymmetrien auf Märkten mit risikobehafteten Produkten und mit Sicherheitsgütern

Bei der Ableitung der Nachfragefunktion nach Sicherheitsmaßnahmen wurde implizit unterstellt, daß die Individuen über die einzelnen Nachfragedeterminanten vollständig informiert sind. Im Gegensatz zum vorangegangenen Abschnitt, in welchem Ursachen für einen „falschen“ funktionalen Zusammenhang zwischen den Determinanten und der optimalen Menge untersucht wurden, beschäftigt sich dieser Abschnitt damit, warum und in welchem Ausmaß Unkenntnis über die einzelnen Nachfrageparameter zu Allokationsineffizienzen führen kann. Hierbei muß folgende Unterscheidung getroffen werden. Die Kenntnisse über die Parameter, welche die Höhe des Erwartungsschadens beeinflussen, werden durch das Bewußtsein über das bei der Nutzung von Produkten immanente Schadenpotential bestimmt, während die Informationslage über die Effizienz von Sicherheitsvorkehrungen durch die Situation auf den Märkten für Sicherheitsgüter beeinflußt wird. Dies bedeutet, daß die Informationsverteilung sowohl auf den Märkten risikobehafteter Produkte als auch für Sicherheitsmaßnahmen analysiert werden muß.

Asymmetrische Informationsverteilung bezeichnet den Zustand, in welchem die "Marktpartner [...] über einen ungleichen Zugang zu [den für die Markttransaktion] relevanten Daten verfügen."[145] Es lassen sich grundsätzlich zwei Arten von Informationsmängeln unterscheiden.[146] Zum einen spricht man von Unkenntnis, wenn die Wirtschaftssubjekte unzureichend über Qualität, Nutzen und Preis eines Pro-

[145] Meyer (1990), S. 105. Nach Meyer können Informationsasymmetrien auch als Ursache für externe Effekte verstanden werden, weil sie durch opportunistische Verhaltensweisen zu einem Auseinanderfallen von Leistung und Gegenleistung führen können. Vgl. zur asymmetrischen Information auch Spremann (1990), S. 561-586.

[146] Vgl. allgemein zu Marktversagen durch Informationsmängel Fritsch, Wein und Ewers (1993), S. 185-215, und speziell zu Marktversagensursachen wg. Qualitätsunsicherheit Rapold (1988), S. 14-19, und Vahrenkamp (1991), S. 39-42.

duktes informiert sind, zum anderen kann zusätzlich Unsicherheit vorliegen, wenn zukünftige Entwicklungen nicht mit Sicherheit vorausgesagt werden können.[147]

Preisunkenntnis, die durch unvollkommene Markttransparenz i. d. R. bei allen Güterarten vorliegt, wird als Marktversagensursache nicht weiter untersucht. Unwissenheit bzgl. des Nutzens eines Gutes läßt sich zum einen auf das im vorangegangenen Abschnitt bereits diskutierte irrationale Konsumentenverhalten zurückführen.[148] Zum anderen wird Nutzenunkenntnis verursacht, wenn sich der ganze Nutzen eines Gutes erst im Laufe des Nutzungszeitraumes entfaltet. Dabei fällt die Einschätzung bzgl. der Nutzenstiftung um so schwerer, je weiter sie in der Zukunft liegt und je abstrakter und immaterieller ihr Charakter ist.[149] Im Kontext von Sicherheitsmaßnahmen liegt Nutzenunkenntnis dann vor, wenn die Wirtschaftssubjekte nur unvollständig einschätzen können, welche Verluste sie im Schadensfall hinnehmen müssen, bzw. wenn ihnen überhaupt nicht bewußt ist, daß sie eigentlich Bedarf an Präventionsmaßnahmen haben. Dies bedeutet, daß in ihrem Entscheidungskalkül sowohl die Schadenhöhen unterschätzt als auch nicht alle Schadensarten erfaßt werden. Die Nachfrage nach Sicherheitsgütern und -maßnahmen entspricht dann nicht dem ökonomisch effizienten Niveau, weil der antizipierte Erwartungsschaden geringer ist als der tatsächliche.

Dieselbe Wirkung kann aber auch durch die Qualitätsunkenntnis bei risikobehafteten Produkte eintreten, wenn der Erwartungsschaden, den die Nutzung eines risikobehafteten Gutes mit sich bringt, falsch eingeschätzt wird. Im Gegensatz zum Informationsdefizit der Nachfrager bei Nutzenunkenntnis liegt bei Qualitätsunkenntnis im allgemeinen eine asymmetrische Informationsverteilung zwischen Nachfrager und Anbieter vor.[150] Die traditionelle neoklassische Annahme homogener Güter kann deshalb für viele risikobehaftete Produkte nicht aufrechterhalten

---

[147] Schulenburg (1993), S. 515, unterscheidet zwischen Marktunsicherheit, welche unvollständige Informationen über den Güterraum, die Gutseigenschaften und die Preise umfaßt, und technologischer Unsicherheit als Ungewißheit bzgl. der Zukunft. Die Versicherungsmärkte, die gerade durch Unsicherheit begründet sind, wurden bereits in Abschnitt 1.3.4 hinsichtlich spezieller Marktversagensgründe durch Ungewißheit analysiert und werden nicht noch einmal aufgenommen.

[148] Bei Nutzenunkenntnis handelt es sich eigentlich um ein im Nachfrager immanentes Informationsdefizit und nicht um die noch folgende asymmetrische Informationsverteilung zwischen den Marktseiten.

[149] Einschlägige Beispiele für Güter, bei denen Nutzenunkenntnis vorliegt und die deshalb z. T. als meritorische Güter vom Staat bereitgestellt werden, sind Bildungs- und Gesundheitsinvestitionen.

[150] Vgl. dazu besonders Fritsch, Wein und Ewers (1993), S. 186-193. Milde (1988), S. 2, grenzt gegen die asymmetrische Informationsverteilung noch zwei weitere Fälle ab. Symmetrische Informationsverteilung liegt vor, wenn beide Marktseiten entweder gleich vollkommen oder gleich unvollkommen über die Produkteigenschaften informiert sind.

werden, weil die Nachfragerseite meistens nicht vollständig über deren heterogenes Schadenpotential informiert ist. Selbst die Vorgehensweise, diese Produkte als Erfahrungsgüter zu betrachten, welche in der Nutzungszeit ihr Schadenpotential offenbaren, ist in vielen Fällen nicht korrekt. Denn sowohl der stochastische Charakter der Problematik als auch die mögliche Nichtentdeckung von eingetretenen Schäden[151] machen den Erwartungsschaden nur schwer bestimmbar. Die Unkenntnis über Schadenpotentiale bei der Nutzung risikobehafteter Produkte kann also erhebliche Fehlallokationen auslösen, weil tendenziell in vielen Fällen durch die Unterschätzung von Risiken die Nachfrage nach Sicherheitsmaßnahmen zu gering ausfällt.[152]

Analog zur Informationsasymmetrie bzgl. Produkten mit Risikopotentialen muß auch auf den Märkten für Sicherheitsmaßnahmen die traditionelle neoklassische Annahme homogener Güter aufgegeben werden, weil die Nachfragerseite nicht vollständig über die heterogenen Qualitätseigenschaften informiert ist.[153] Selbst das etwas weniger stringente Konzept des Erfahrungsgutes, nach welchem der Nutzer einen Erfahrungsgewinn bzgl. der Produktqualität im Laufe des Nutzungszeitraumes erfährt, trifft auf Sicherheitsvorkehrungen nicht zu. Denn Vorsichtsmaßnahmen haben den Charakter von Glaubens- oder Vertrauensgüter, welche sich dadurch auszeichnen, daß sie sich erst im Schadensfall bzw. bei seiner Verhinderung bewähren können.[154] Deshalb sind die Nachfrager beim Erwerb nicht zu einer objektiven Bewertung der Wirksamkeit von Schadenpräventionsgütern fähig. Dies liegt zum einen an der stochastischen Komponente des Entscheidungsproblems und zum anderen am Unvermögen der Wirtschaftssubjekte die Reduktion des Erwartungsschadens den Sicherheitsvorkehrungen zuzuordnen.[155] Es herrscht also Un-

---

[151] Dieser Aspekt spielt besonders bei der Informationssicherheit eine wichtige Rolle und wird deshalb in Abschnitt 2.6.2.2 der Fallstudie genauer analysiert.

[152] Bei Innovationen kann die Unsicherheit über das Risikopotential so groß sein, daß eine Marktetablierung aufgrund zu hoher Sicherheitsausgaben nicht gelingt.

[153] Im Grunde muß die asymmetrische Informationsverteilung noch genauer differenziert werden. Denn die Kenntnis der Anbieter von Sicherheitsvorkehrungen über deren Effizienz basiert auf Erfahrungswerten, welche sich nicht unbedingt auf zukünftige Entwicklungen extrapolieren lassen. Jedoch liegt immer noch ein Erfahrungsvorsprung gegenüber den Konsumenten vor, so daß weiterhin von einer asymmetrischen Informationsverteilung ausgegangen werden kann. Vgl. dazu auch Abschnitt 2.6.2.2 der Fallstudie.

[154] Blankart & Pommerehne (1985), S. 439f, begründen auch damit, daß Vertrauensgüter, wie die Rechtsprechung und die Streitkräfte, nicht zur Privatisierung geeignet sind, weil die Qualität der Leistungserstellung nicht erfaßbar ist und die Sorgfalt letzterer nur an der Beachtung bestimmter Regeln gemessen werden kann.

[155] Die Nachfrager unterliegen also einem Informationsdefizit, aufgrund dessen die von ihnen antizipierten Produktivitäten von s bzgl. Schadenhöhe und Schadeneintrittswahrscheinlichkeit, d. h. $p'(s)$ und $L'(s)$, nicht mit den wahren Werten übereinstimmen. Im engen Zusammenhang damit steht das

kenntnis über die Effizienz bzw. die Grenzproduktivität der Sicherheitsmaßnahmen. Eine Überschätzung dehnt die Nachfrage übermäßig aus, während bei einer Unterschätzung zu wenig Prävention ergriffen wird. In beiden Fällen kommt es zu Allokationsineffizienzen und damit zu gesellschaftlichen Wohlfahrtseinbußen.

Zusätzlich zu den aus der statischen Analyse abgeleiteten Ineffizienzen muß betrachtet werden, welche Entwicklungen sich auf dem Markt für Sicherheitsgüter durch die Informationsasymmetrien ergeben.[156] Bisher wurde das Angebot an Schadenpräventionsgüter, welches sich durch die unterschiedlichen Wirksamkeiten bzgl. der Reduktion der Schadeneintrittswahrscheinlichkeit und der Schadenhöhe differenzieren läßt, als exogen angenommen. Jedoch werden die Anbieter auf das Informationsdefizit der Nachfrager, welches dazu führt, daß diese durchschnittlich effektive Sicherheitsmaßnahmen zu einem entsprechenden Durchschnittspreis nachfragen, reagieren, indem der qualitativ hochwertige und kostenintensive Teil des heterogenen Angebotes aufgrund des nicht kostendeckenden Durchschnittspreises aus dem Markt verdrängt wird. Dieser Prozeß der adversen Selektion[157] führt wiederum auf der Nachfrageseite zu einem Rückgang der Zahlungsbereitschaft, so daß langfristig nur noch die geringste Qualität angeboten und nachgefragt wird.[158] Das Marktversagen besteht nun darin, daß es sowohl für die Nachfrager als auch für die Anbieter besonders wirksamer Schadenpräventionsgüter eine Wohlfahrtssteigerung bedeuten würde, wenn Transaktionen in diesem Marktsegment zustande kommen würden.

Falls man im Gegensatz zur adversen Selektion mit exogenen, nicht beobachtbaren Qualitäten annimmt, daß die Anbieter das Qualitätsniveau selbst bestimmen können, tritt das Moral-Hazard-Phänomen auf den Märkten für Sicherheitsvorkehrungen auf.[159] Denn die Anbieter haben den Anreiz, eine schlechtere und damit auch kostengünstigere als von den Nachfragern antizipierte Qualität zu produzieren, um einen höheren Gewinn zu erzielen. Der Anreiz eines Anbieters zu Moral Hazard ist

---

in FN 138 vorgebrachte Argument, daß die Wirtschaftssubjekte glauben, die Effizienz der Sicherheitsvorkehrungen überdurchschnittlich steigern zu können.

156 Eigentlich müßte auch die Dynamik auf den Märkten für risikoreiche Güter analysiert werden. Deren Konstellation wurde aber bei Analyse der Allokationsoptima in Kapitel 1.2 als exogen unterstellt.

157 Vgl. dazu die Beiträge von Akerlof (1970), S. 488-500, Wilson (1980), S. 108-130, Kim (1985), S. 836-843, und u.a. Milde (1988), S. 1-6.

158 Vgl. dazu auch Hauser (1979), S. 741f.

159 Der Anreiz zu Moral Hazard von seiten der Anbieter ist auch dann besonders groß, wenn die Qualitätsreduktion ohne hohen Aufwand möglich ist. Bei technischen Sicherheitssystemen ist dieser im allgemeinen eher hoch. Im Fall von Dienstleistungen, wie Wach- und Sicherheitsdiensten, kann die Qualität dagegen nahezu kostenlos gesenkt werden.

um so größer, je weniger negative Sanktionsmöglichkeiten die Nachfrager ihm gegenüber haben, d. h. je unempfindlicher und verzögerter sie auf die schlechtere Qualität reagieren und je kleiner seine Umsatzeinbußen durch den Rückgang der Nachfrage und der Zahlungsbereitschaft sind. Analog zu dem extremen Ergebnis der adversen Selektion kann sich bei hinreichend ungleicher Informationsverteilung zuungunsten der Nachfrager ein Marktgleichgewicht einstellen, in welchem nur noch das schlechteste Qualitätsniveau umgesetzt wird.

Adverse Selektion und Moral Hazard auf dem Markt für Sicherheitsgüter und -maßnahmen tragen also bei starken Informationsasymmetrien beide dazu bei, daß das Angebot und dadurch auch die Nachfrage nach qualitativ hochwertigen und effizienten Sicherheitsmaßnahmen aus dem Markt gedrängt werden.[160] Jedoch muß zusätzlich zur durchschnittlich angebotenen Qualität der Sicherheitsvorkehrungen auch der ursprünglich als exogen unterstellte Grad der Informationsasymmetrie endogenisiert werden, denn alle Wirtschaftssubjekte, welche hohe Qualitäten entweder anbieten oder nachfragen wollen, haben aufgrund zu erwartender Wohlfahrtsgewinne einen Anreiz, die bestehenden Informationsineffizienzen zu beseitigen.

Deshalb kann der Marktmechanismus eigenständig zum Abbau der Informationsasymmetrien beitragen, indem die schlecht informierte Marktseite versucht, zusätzliche Informationen zu gewinnen ("Screening"), und die besser informierte Marktseite sich bemüht, glaubwürdige Informationen über die Qualität ihrer Produkte zu verbreiten ("Signaling").[161] Unter welchen Bedingungen es dadurch zu einem Abbau der Informationsdefizite kommen kann und warum sich dennoch nicht Informationssymmetrie zwischen den Marktseiten einstellen wird, soll Gegenstand des nächsten Abschnittes sein.

---

160 Eine weitere Art von Marktversagen durch Moral Hazard wird im Zusammenhang mit Schadenpräventionsgütern dann relevant, wenn die Anbieter eine Sicherheitsgarantie für die Wirksamkeit ihrer Produkte geben und die Nachfrager den Anreiz und die Möglichkeit haben, den Garantiefall ohne Identifikationsmöglichkeit ihrer Mitschuld eintreten zu lassen. Dies werden die Anbieter in ihre Kostenkalkulation miteinberechnen und dementsprechend den Preis für Schadenverhütung erhöhen. Die Folge der Preiserhöhung ist, daß vertragstreue Individuen ihre Nachfrage reduzieren, obwohl es für sie selbst und für die Anbieter wohlfahrtssteigernd wäre, wenn es zu Markttransaktionen in größerem Umfang käme. Vgl. zum sogenannten doppelten Moral Hazard Vahrenkamp (1991), S. 82-89

161 Die Verbreitung von Informationen über die Eigenschaften eines Produktes durch die Anbieter kann auch dazu beitragen, die Nutzenunkenntnis der Nachfrager bzw. die asymmetrische Informationsverteilung auf den entsprechenden Märkten für risikobehaftete Produkte abzubauen. Auf die Rückwirkungen des Signaling und des Screening in Sicherheitsmärkten auf andere Produktmärkte wird jedoch nicht weiter eingegangen.

1.4.4 Ineffizienzen beim Abbau der Informationsasymmetrien auf den Märkten für Sicherheitsgüter

Da sowohl der Anbieter- als auch der Nachfragerseite durch das Informationsdefizit bzgl. der Qualität der Sicherheitsvorkehrungen Wohlfahrtseinbußen entstehen, existieren in beiden Gruppen Anreize, diese Informationsasymmetrien abzubauen.[162]

Die relativ schlechter informierte Marktseite hat die Möglichkeit, über die Beschaffung von Informationen über die Produkteigenschaften ("Screening") ihre Informationslage zu verbessern. Zum einen kann das Wirtschaftssubjekt seinen Kenntnisstand durch eigene Recherchen zu vervollkommnen suchen, bis der erwartete Nutzenzuwachs weiterer Qualitätsinformationen größer als die zusätzlich anfallenden Suchkosten ist.[163] Dieser Vorgehensweise sind Grenzen gesetzt, wenn es der besser informierten Marktseite möglich ist, entscheidende Informationen geheimzuhalten, und wenn die Kosten der Informationsbeschaffung prohibitiv hoch sind, weil u. U. gewisse Spezialkenntnisse mit hohem Fixkostenaufwand benötigt werden. Bezogen auf die Eigenschaften von Sicherheitsvorkehrungen können beide Tatbestände erfüllt sein, weil es sich für gewöhnlich zum einen um technisch komplexe Systeme handelt, deren Effizienz sich erst in Schadensfällen bzw. bei deren Verhinderung bewähren kann, und es deshalb zum anderen den Anbietern nicht schwer fällt, die entsprechend relevanten Informationen geheimzuhalten.[164]

Deshalb müssen sich die Individuen an Spezialisten wenden, welche die Voraussetzungen zur Informationsbeschaffung oder gar die nachgefragten Kenntnisse schon besitzen. Jedoch haben Informationen folgende spezielle Eigenschaften, welche das Entstehen eines effizienten Angebotes an Informationen verhindern können.[165]

Bei Informationen besteht das Problem, daß auch Nichtzahler mit geringem Aufwand an der Information partizipieren können. Durch die Nicht-Ausschließbarkeit

---

[162] Ähnliche Anreize und Lösungsmöglichkeiten bestehen bei Informationsasymmetrie hinsichtlich der Schadenspotentiale auch auf den Märkten für risikobehaftete Produkte, welche aber in diesem Kontext nicht weiter berücksichtigt werden. Vgl. zu den Lösungsmöglichkeiten Fritsch, Wein und Ewers (1993), S. 193-198. Meyer (1990) nimmt eine andere Systematisierung vor und unterteilt die Lösungsmöglichkeiten nach Informationsbereitstellung, Risikoteilungssysteme, duale Märkte und vertikale Integration.

[163] Vgl. zu Suchstrategien der Konsumenten die theoretische Analyse von Nelson (1970), und den Vergleich in Schulenburg (1993), S. 524f.

[164] Auf diese Problematik wird genauer in der Fallstudie eingegangen.

[165] Vgl. Gruenspecht & Lavé (1989), S. 1527, W. Kip Viscusi (1984), S. 5f, Beales, Craswell und Salop (1981), S. 503-506, Vahrenkamp (1991), S. 36-38, und Magoulas (1985), S. 28-32.

kann der Informationsanbieter aber nicht den gesamten ökonomischen Wert seiner Kenntnisse vereinnahmen, weil jeder Käufer zu einem potentiellen Konkurrenten wird, der die Information anderen möglichen Interessenten weiterverkaufen kann.[166]

Falls die Verbreitung der Information durch die Käufer unterbunden werden kann, d. h. ein Ausschluß von Free-Ridern möglich ist, ergibt sich aufgrund der geringen Verbreitungskosten eine zweite Ursache für ineffiziente Marktergebnisse. Denn es handelt sich bei der Publikation einer bereits erstellten Information um ein natürliches Monopol.[167] Deshalb kann die Auskunft zur Deckung der durch die Informationsgenerierung verursachten Fixkosten nur weit über dem Preis angeboten werden, welcher dem Grenzkostenniveau in Form der geringen Verbreitungskosten entspricht, so daß das Volumen der transferierten Informationen suboptimal sein wird. Denn um Paretoeffizienz zu erreichen, darf die Information eigentlich nur zu einem Preis abgegeben werden, der die Kosten der Informationsträger und der Verbreitung deckt. Dies kann aufgrund der dadurch resultierenden negativen Gewinne für die Informationsanbieter aber nicht ohne staatliche Intervention realisiert werden.

Schließlich besteht vor dem Hintergrund des Informationsparadoxons von seiten der Nachfrager Unsicherheit darüber, welchen Nutzen ihnen die erworbene Information einbringen wird bzw. welche Qualität sie hat, so daß sie bei Risikoaversion im Zweifel auf eine Informationsbeschaffung verzichten werden.[168]

Diese Eigenschaften haben zur Folge, daß entweder aufgrund der unzureichenden Ausschließbarkeit der Nichtzahler von der Informationsnutzung sich überhaupt kein Spezialist bereit findet, Informationen über Sicherheitsvorkehrungen anzubieten, oder bei der Möglichkeit zum Ausschluß von den einzelnen Individuen unter volkswirtschaftlichen Gesichtspunkten zu wenig Informationen nachgefragt werden. Die Konsequenz für den Schadensgütermarkt ist, daß aufgrund der unzureichenden Informationsbereitstellung die Unkenntnis über die Qualitätseigenschaften

---

[166] Vgl. Asch (1988), S. 50f.

[167] Magoulas (1985), S. 30f, begründet den fallenden Grenzkostenverlauf der Informationsbereitstellung durch die hohen Fixkosten, welche bei der Produktion anfallen, und mit den relativ niedrigen variablen Kosten der Informationsverbreitung.

[168] Vgl. dazu Hirshleifer & Riley (1992), S. 273f u. Asch (1988), S. 51. Vgl. zur Qualitätsunsicherheit Beales, Craswell und Salop (1981), S. 505.

der Sicherheitsmaßnahmen nicht auf das volkswirtschaftlich effiziente Maß reduziert wird.[169]

Neben den gemeinhin relativ schlechter informierten Nachfragern haben auch die Anbieter von Sicherheitsmaßnahmen einen Anreiz, Informationen direkt und freiwillig den Nachfragern zur Verfügung zu stellen.[170] Da Informationen über ein Produkt fast immer auch durch den eigentlichen Produktionsprozeß entstehen, erscheint deshalb der Abbau der Informationsasymmetrien durch die Anbieterseite als die kostengünstigere Strategie.[171] Jedoch sind bezüglich der Glaubwürdigkeit der Produzenten erhebliche Zweifel angebracht, weil sie bedingt durch die Konkurrenzsituation auf dem Produktmarkt stets einen Anreiz haben, ihre Produktinformationen zu "beschönigen" bzw. falsche Behauptungen aufzustellen.[172] Neben der Qualität der direkten Informationsbereitstellung kann auch ihr Ausmaß volkswirtschaftlich unzureichend sein.[173] Es können nämlich positive Externalitäten für die Mitkonkurrenten auftreten, wenn die Konsumenten die Eigenschaften der Produkte einer Anbietergruppe und nicht dem informierenden Anbieter zuordnen. Dann profitieren von der Nachfragesteigerung durch die Informationspolitik eines Anbieters alle anderen Anbieter, ohne daß ersterer dafür entschädigt wird.[174]

Wirksamer als die direkte Informationsbereitstellung in Form von Werbung sind bzgl. vieler Produkte indirekte, implizit in der Vermarktung und in der Vertragsausgestaltung integrierte Strategien. Hier muß hinsichtlich der Nutzungsdauer der Produkte unterschieden werden. Zunächst wird bei kurzlebigen Gütern auf die Goodwill-Strategie zum Aufbau einer Reputation[175] und anschließend bei langlebigen Produkten auf die Gewährung von Garantieleistungen von seiten der Anbieter eingegangen.

---

169 Es werden insbesondere zu wenig Informationen bzgl. der Effizienz der Sicherheitsmaßnahmen hinsichtlich ihrer Fähigkeit, den Erwartungsschaden zu reduzieren, nachgefragt, so daß die Unsicherheit darüber zu hoch ist und aufgrund risikoaverser Konsumenten, die unternommenen Sicherheitsmaßnahmen zu gering ausfallen werden.

170 Vgl. dazu Rapold (1988), Kapitel 2, welcher verschiedene Möglichkeiten von Goodwill-Strategien aufzeigt. Neben Preisstrategien dient auch der Werbeaufwand als Qualitätssignal. Vgl. dazu u. a. Vahrenkamp (1991), S. 54-65.

171 Vgl. dazu Magoulas (1985), S. 32.

172 Besonders bei Sicherheitssystemen können sich die Anbieter mit dem Hinweis auf die Bedeutung der stochastischen Einflußgrößen und einer in der Realität nicht realisierbaren 100%-Sicherheit ohne schwerwiegende Konsequenzen für das Versagen der Sicherheitsgüter entschuldigen.

173 Es kann aber unter bestimmten Umständen auch zu einem „overinvestment“ in Werbesignale kommen. Vgl. dazu u. a. Beales, Craswell und Salop (1981), S. 507.

174 Vgl. dazu Viscusi (1984), S. 5.

175 Reputationsstrategien sind deshalb möglich, weil die Konsumenten aus vergangenen Erfahrungen mit der Qualität eines Gutes auf das zukünftige Qualitätsniveau schließen.

Anbieter höherer Produktqualitäten können den Reputationsmechanismus dazu nutzen, sich dauerhaft im Markt zu etablieren, indem sie in einer Einführungsphase ihre kostenintensiven Produkte zum Durchschnittspreis anbieten. Die Konsumenten werden die relativ hohe Produktqualität erkennen, und diejenigen mit einer ausgeprägten Präferenz und Zahlungsbereitschaft werden auch bei langfristig höheren Preisen, welche den Produktionskosten einer höheren Qualität entsprechen, eine positive Konsumentenrente realisieren. Der Wiederholungskauf von Erfahrungsgütern, welcher v. a. von der antizipierten Produktqualität abhängig ist, zwingt die Anbieter, die einmal bereitgestellte Qualität weiter bereitzustellen, da sie sonst ihre Reputation bei den Nachfragern verlieren.[176] Das erworbene Ansehen hat die Eigenschaft einer Investition, welche es ermöglicht, trotz der Gefahr adverser Selektion hohe Qualität profitabel abzusetzen. Bei Lieferung von unerwartet schlechter Qualität droht ein Reputationsverlust und damit ein Nachfragerückgang. Der Anreiz zum Aufbau einer Reputation ist aber nur dann gegeben, wenn es sich um Produkte handelt, welche wiederholt gekauft werden und deren Qualität sich nach dem Kauf leicht feststellen läßt. Da es sich bei Schadenpräventionsgütern nicht um Erfahrungsgüter handelt, sondern um Vertrauensgüter, welche i. d. R. nur einmalig erworben werden und deren Effizienz sich nur im Schadensfall offenbaren kann, ist es selbst für Anbieter mit einem längerfristigen Zeithorizont nicht immer lukrativ, sich eine zeitintensive und kostspielige Reputation aufzubauen, weil die Erträge aus kurzfristigen Täuschungsmanövern gegenüber den schlechter informierten Nachfragern sehr viel höher sind als die Erträge einer langfristig angelegten Reputationsstrategie.[177]

Eine häufig angewandte Strategie der Anbieter von langlebigen und nur einmal erworbenen Gütern ist die Gewährung von überdurchschnittlichen Garantieversprechen, welche eine hohe Qualität der angebotenen Produkte signalisieren.[178] Jedoch ist ein Garantieversprechen irrelevant, wenn nur das sorgfältige Bemühen aber nicht der Erfolg garantiert wird. Dies trifft auch auf Sicherheitsmaßnahmen zu, denn eine Garantie auf 100% Sicherheit wird kein Anbieter geben können.[179] Die

---

176 Vgl. dazu die theoretischen Analysen von Leffler & Klein (1981) und Shapiro (1983).

177 Vgl. zu den dafür geltenden Bedingungen Rapold (1988), S. 51.

178 Dieser Vorgehensweise sind allerdings Grenzen gesetzt, wenn der Abnehmer unbeobachtet den Schadensfall herbeiführen kann und den entstandenen Schaden beim Anbieter einzuklagen versucht. Diese Möglichkeit besteht durchaus bei Sicherheitsgütern, da ihre Effizienz immer auch von der sorgfältigen Handhabung der Konsumenten abhängt.

179 Dies liegt daran, daß in der Realität kein geschlossener Wahrscheinlichkeitsraum mit der Kenntnis aller Risikoarten vorliegt. Sicherheitssysteme sind aber nur auf die Abwehr bestimmter, bereits ex ante bekannter Risikoarten ausgerichtet. Deshalb können Schadensfälle nicht ganz ausgeschlossen

Gewährleistung, daß die Schadenprävention in 99% der Fälle erfolgreich ist, kann aber i. d. R. nicht überprüft werden, weil ex post nicht mehr mit Eintrittswahrscheinlichkeiten argumentiert werden kann.

"Screening" und "Signaling" als substitutive und komplementäre Strategien der Marktteilnehmer zur Beseitigung von Informationsasymmetrien auf Produktmärkten sind Restriktionen unterworfen, welche besonders für den Markt für Sicherheitsgüter charakteristisch sind. Die technische Komplexität der Sicherheitssysteme und die geringe Profitabilität der privaten Vermarktung von Informationen über Sicherheitssysteme lassen die „Screening“-Strategie der Nachfrager als wenig geeignetes Instrument für den Abbau der Informationsasymmetrien erscheinen. Das „Signaling“ der Anbieter ist im Falle von Sicherheitsvorkehrungen maßgeblichen Beschränkungen unterworfen, weil die direkte Informationsbereitstellung einen geringen Grad an Glaubwürdigkeit aufweist, der Anreiz zum Aufbau einer Reputation aufgrund ihrer Langlebigkeit gering ist und die Einräumung von Garantieversprechungen infolge unzureichender Einklagbarkeit die Nachfrager nicht überzeugen wird. Die Eigeninitiative der Wirtschaftssubjekte reicht deshalb nicht aus, um die Informationsineffizienzen auf ein effizientes Niveau zu senken, und es müssen zusätzlich staatliche Regelungen ergriffen werden, die sowohl den Informationsfluß zwischen den Marktseiten erleichtern als auch seine Glaubwürdigkeit erhöhen.[180]

1.4.5 Allokationsineffizienzen durch Externalitäten von Sicherheitsgütern und -maßnahmen

Die letzte und bedeutendste Ursache für nachfragebedingte Allokationsineffizienzen auf den Märkten für Sicherheitsgüter und -maßnahmen sind Externalitäten. Im allgemeinen spricht man dann von externen Effekten, wenn in die Produktions- oder Nutzenfunktion eines Individuums außer seinen eigenen Aktionsparametern mindestens ein Faktor eingeht, welcher nicht von ihm selbst kontrolliert wird.[181] Jedoch liegt eine allokative Ineffizienz bzw. Marktversagen nur dann vor, wenn es sich um sogenannte technologische Externalitäten handelt. Preisänderungen oder

---

und die Schadenhöhen nicht kalkuliert werden, so daß die Garantie auf hundertprozentige Sicherheit für den Anbieter zum untragbaren Risiko wird.

180 In Kapitel 1.5.1 wird deshalb auf informationspolitische Instrumente eingegangen. Vgl. dazu Fritsch, Wein und Ewers (1993), S. 199f, und Magoulas (1985), S. 42.

181 Vgl. Fritsch, Wein und Ewers (1993), S. 54.

pekuniäre externe Effekte, welche durch Verschiebung von Angebots- oder Nachfrageparametern verursacht werden, sind Ausdruck eines funktionierenden Marktmechanismus und eine notwendige Bedingung für eine effiziente Ressourcenallokation.

In der folgenden Analyse werden deshalb nur die durch technologische Externalitäten ausgelösten Allokationsineffizienzen, welche durch einen direkten physischen Zusammenhang zwischen den Produktions- und Nutzenfunktionen mehrerer Wirtschaftssubjekte ohne gleichzeitige marktmäßige Kompensation dieser Interdependenzen gekennzeichnet sind, dargestellt.[182] Die Auswirkung deren Existenz ist, daß die privaten Kosten bzw. Nutzen von den für die Gesamtgesellschaft relevanten sozialen Kosten oder Nutzen im Ausmaß der externen Effekte auseinanderfallen. Dies bedeutet, daß die relativen Marktpreise nicht die volkswirtschaftlichen Knappheiten widerspiegeln und dadurch eine ineffiziente Ressourcenallokation verursachen. Technologische Externalitäten können zum einen sowohl beim Konsum als auch bei der Produktion auftreten, und zum anderen sowohl positive als auch negative Wirkungen auf Dritte haben.[183] Im folgenden werden die verschiedenen Quellen von Ineffizienzen dargestellt, welche im Zusammenhang mit Sicherheitsmaßnahmen auftreten können.[184]

Untersucht man den Schadensfall, der durch eine mit positiven Schadenswahrscheinlichkeiten behaftete Aktivität eines Wirtschaftssubjektes - sei es ein Produzent oder ein Konsument - hervorgerufen wird, werden die anfallenden Kosten oft nicht nur vom involvierten Individuum - Konsument oder Produzent - getragen, sondern es werden auch Dritte entweder unmittelbar oder indirekt betroffen, indem die Gemeinschaft als ganzes für einen Teil der Schäden aufkommt.[185] Beispielsweise werden bei einen Autoverkehrsunfall i. d. R. neben dem Lenker des Unfallwagens weitere Individuen tangiert. Abstrahiert man zunächst von der Existenz eines Haftungssystems, dann trägt der Schadenverursacher den Gesamtschaden nicht alleine, sondern den übrigen Opfern fällt jeweils der sie betreffende Teil des kompletten Schadens zu. Diese Wirkungen einer Tätigkeit, die einen Schaden verursacht, bezeichnet man als negative technologische externe Effekte. Selbst bei ef-

---

182 Vgl. ebenda, S. 55-65, und die anspruchsvolle Darstellung von Cornes & Sandler (1986), 29-66.

183 Vgl. dazu die verschiedenen Beispiele in Fritsch, Wein und Ewers (1993), S. 57f, und in Arnould & Grabowski (1981), S. 29, bzgl. Autounfällen.

184 Unter die Produktionsexternalitäten fallen u. a. die ökonomischen Wirkungen von Arbeitsunfällen. Vgl. dazu den Beitrag von Oi (1974), S. 669-699, und eine theoretische Analyse von Hiebert (1983), S. 160-168.

185 Vgl. dazu Spengler (1968), S. 632f, u. Gruenspecht & Lavé (1989), S. 1523.

fektiv funktionierenden Haftungsregeln[186], welche theoretisch negative Externalitäten verhindern sollten, sprechen zwei Gründe dafür, daß durch einen Schadensfall, der nicht nur den Verursacher betrifft, trotzdem Kosten entstehen, die entweder die Gruppe der Opfer oder die Gesellschaft als ganzes zu tragen hat. Erstens werden bei einem Unfall in aller Regel auch immer immaterielle Werte tangiert, welche monetär nicht entgolten werden oder durch Geldeinheiten nicht zu ersetzen sind.[187] Und zweitens müssen zur Bestimmung des Verursachers und der Kompensationszahlungen Informations- und Transaktionskosten aufgewendet werden, die nur zu einem Teil vom Verlierer eines Rechtsstreites getragen werden, weil das Rechtswesen vor allem durch steuerfinanzierte Staatsausgaben bestritten wird. In sein Kostenminimierungskalkül gehen gerade die nicht kompensierbaren Schadenskomponenten und die der Allgemeinheit entstehenden Verwaltungs- und Justizkosten nicht ein, so daß er aufgrund dieser Externalitäten eine volkswirtschaftlich betrachtet zu geringe Schadenvermeidung betreibt bzw. zu wenig Sicherheitsgüter nachfragt.

Im oben dargestellten Beispiel werden durch die Unterlassung von Sicherheitsvorkehrungen - etwa in Form überhöhter Geschwindigkeit - unmittelbar negative Externalitäten bei anderen Individuen hervorgerufen, welche beim Verursacher in seinen Überlegungen über die Ergreifung von Sicherheitsmaßnahmen in Zusammenhang mit seinen risikoreichen Aktivitäten nicht miteinbezogen wurden. Jedoch existieren auch Konstellationen, in welchen die vom betrachteten Individuum getroffenen Schadenpräventionsmaßnahmen die Schäden bzw. Schadenswahrscheinlichkeiten für Dritte indirekt reduzieren, so daß es dadurch positive externe Effekte auslöst, für die es nicht kompensiert wird.[188] Beispielsweise kann die individuelle Grippeimpfung dazu beitragen, daß das Ansteckungsrisiko für die Mitmenschen zurückgeht und diese dadurch eine höhere Produktionsleistung erreichen. Zwar hat der einzelne durch die Verringerung seiner Krankheitswahrscheinlichkeit einen

186 Vgl. Abschnitt 1.5.3 zu einer differenzierten Darstellung verschiedener Haftungsregeln und ihren allokativen und distributiven Wirkungen. Vgl. zu weiteren Unvollkommenheiten des Haftungsrechtes Cansier (1993), S. 254-261.

187 So können z. B. Arzneimittel Schäden an Leib und Leben verursachen, die materiell nicht vollständig abgegolten werden können. Dieselbe Problematik gilt auch für die Verletzung der Vertraulichkeit von Kommunikationsinhalten und wird deshalb in der Fallstudie ausführlich diskutiert.

188 Positive Externalitäten treten deshalb auf, weil der dem privaten Optimierungskalkül unterliegende Erwartungsschaden geringer ist als der tatsächlich der Volkswirtschaft entstehende. Entsprechend kann auch argumentiert, daß bei riskanten wirtschaftlichen Aktivitäten negative Externalitäten auftreten. Jedoch konzentriert sich diese Arbeit auf die Allokationsineffizienzen bei der Ergreifung von Sicherheitsmaßnahmen, so daß letztere Betrachtungsweise und damit geeignete Lösungsmöglichkeiten in Form der Besteuerung schadensverursachender Produkte nur begrenzt berücksichtigt wird.

Nutzengewinn, dabei erzeugt er aber bei seiner Umgebung auch positive externe Effekte, für die er nicht kompensiert wird. In diesem Fall ergreift das Individuum Vorsichtsmaßnahmen, welche zwar für ihn wohlfahrtssteigernd sind, aber auch das Nutzenniveau der anderen positiv beeinflussen.[189]

Abbildung 5 stellt sowohl die dargelegten positiven als auch die negativen externen Effekte als eine durch Rechtsverschiebung der privaten Grenznutzenkurve generierte soziale Grenznutzenkurve dar, welche sowohl die privaten als auch sozialen Nutzenkomponenten der Sicherheitsmaßnahmen umfaßt. Es zeigt sich, daß ohne staatliche Intervention in die Märkte für Sicherheitsgüter unter volkswirtschaftlichen Effizienzgesichtspunkten zu wenig Schadensprävention betrieben wird, weil das aus dem privaten Optimierungskalkül heraus gewählte Niveau s^*_{privat} kleiner als das gesellschaftlich effiziente Ausmaß s^*_{sozial} ist. Der Wohlfahrtsverlust kann auch als Fläche des grauen Dreiecks ausgedrückt werden.

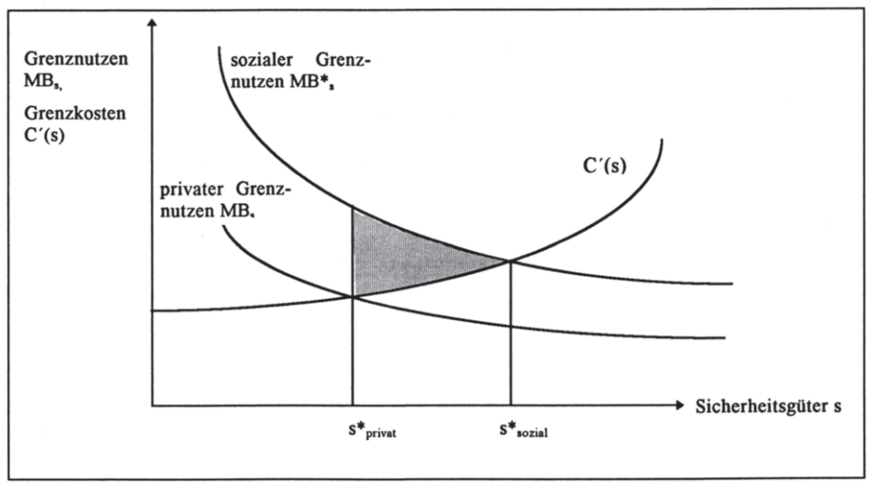


Abb. 5: Externe Effekte von Sicherheitsgütern und -maßnahmen

Bisher wurden Ineffizienzen bei der Allokation von Sicherheitsmaßnahmen vor dem Hintergrund von in ihrem Umfang begrenzten Externalitäten bestimmt. Es können jedoch noch zwei weitere Fälle unterschieden werden. Sind die positiven Externalitäten gar so umfangreich, daß alle Gesellschaftsmitglieder davon einen

---

189 Private Abschreckungsmaßnahmen gegen kriminelle Handlungen können dagegen auch negative Externalitäten verursachen, indem sie die Deliktwahrscheinlichkeit bei den Mitbürgern erhöhen. Vgl. dazu Clotfelter (1978), S. 398.

ähnlich hohen Nutzen haben wie das Wirtschaftssubjekt, das die Sicherheitsvorkehrungen ergreift, dann handelt es sich sogar um ein öffentliches Gut mit den Eigenschaften der Nichtausschließbarkeit von Nichtzahlern und der Nichtrivalität zwischen den Nutzern. Hier kann nur eine staatliche Bereitstellung verhindern, daß ein suboptimales Niveau bzw. überhaupt keine Sicherheitsmaßnahmen ergriffen werden. Ein Paradebeispiel für ein Sicherheitssystem als reines öffentliches Gut ist die nationale Verteidigung. Die einzelnen Individuen haben keinen Anreiz, sich gegen eine militärische Bedrohung durch äußere Feinde zu schützen, weil jeweils die ihnen dadurch entstehenden Kosten weit höher sind als ihre individuellen Nutzen. Aufgrund der Nichtausschließbarkeit wird durch Privatinitiative keine nationale Verteidigung bereitgestellt, obwohl der gesamtwirtschaftliche Nutzen größer ist als die entsprechenden Kosten.[190]

Als dritter Fall neben Sicherheitsmaßnahmen mit begrenzten Externalitäten oder als öffentliches Gut muß noch der Clubgutfall untersucht werden.[191] Entgegen einem reinen öffentlichen Gut zeichnet sich ein Clubgut durch die Freiwilligkeit der Mitgliedschaft, durch die sich ab einer bestimmten Mitgliederzahl einstellende Rivalität in der Nutzung, durch die Möglichkeit des Ausschlusses von Nichtzahlern und die dadurch notwendige simultane Entscheidung über Ausstattung und Mitgliederanzahl aus.[192] Zum Beispiel können Sicherheitsvorkehrungen in einem nichtöffentlichen Verkehrsnetz den Charakter eines Clubgutes haben, denn diejenigen, die sich durch das Entrichten eines Fahrpreises oder einer Benutzungsgebühr Zugang zum Verkehrssystem verschafft haben, kommen alle in gleichem Maße in den Genuß der Verkehrssicherheit.[193] Im Gegensatz zu reinen öffentlichen Gütern entstehen bei Clubgütern keine Allokationsineffizienzen, die eine Intervention in den Markt von seiten des Staates rechtfertigen.[194] Dies gilt jedoch nur, wenn die

---

190 Vgl. allgemein dazu Oakland (1987), S. 514f, und zum Aspekt der Produktsicherheit als öffentliches Gut Asch (1988), S. 44-48, oder Lavé (1968), S. 515f. Die staatliche Bereitstellung von Sicherheitssystemen wird in Abschnitt 1.5.6 dargestellt und bewertet.

191 Vgl. dazu Oakland (1987), S. 502-509, und die ausführliche Darstellung von Cornes & Sandler (1986), Teil IV.

192 Vgl. zu den Eigenschaften Cornes & Sandler (1986), S. 159-161.

193 Neben der Flugsicherheit hat auch die Sicherheit von Kommunikationssystemen den Charakter eines Clubgutes, weil zum einen die Ausschlußmöglichkeit über die Erhebung von Benutzungsgebühren besteht und zum anderen alle Kommunikationsteilnehmer unbedrängt die gleichen Sicherheitseigenschaften der Netze in Anspruch nehmen können, wenn man von der Überfüllungsproblematik einmal absieht.

194 In diesem Kontext wird davon abgesehen, daß ein Monopolist aufgrund von positiven Skalenerträgen das Clubgut anbietet. Denn dann ergeben sich die bekannten Wohlfahrtsverluste eines Monopols in Form von höheren Preisen und geringeren Outputs im Vergleich zur Wettbewerbssituation. Vgl. dazu Oakland (1987), S. 518-522.

Nutzung des Clubgutes durch die Clubmitglieder keine Sicherheitsrisiken beim Rest der Gesellschaft verursacht, denn dann haben die Sicherheitsentscheidungen der Clubmitglieder gesellschaftliche Konsequenzen und es liegen wiederum externe Effekte vor, welche die oben dargestellten Allokationsineffizienzen hervorrufen.[195]

Die Analyse hat gezeigt, daß Sicherheitsmaßnahmen neben begrenzten externen positiven Effekten durchaus die Eigenschaften eines reinen öffentlichen oder eines Clubgutes haben können. Wenn die Allokation ausschließlich dem Markt und der Initiative der Wirtschaftssubjekte überlassen wird, kommt es zu einem volkswirtschaftlich suboptimalen Sicherheitsniveau. In Kapitel 1.5 werden verschiedene Lösungsmöglichkeiten aufgezeigt, die geeignet sind, diese Allokationsineffizienzen zu vermindern bzw. zu beseitigen.

1.4.6 Fazit

In diesem Kapitel wurden die verschiedenen Aspekte von Allokationsineffizienzen identifiziert, welche durch die Nachfrageseite verursacht werden. Es lassen sich tendenziell folgende Ergebnisse feststellen:

1. Irrationales Nachfragerverhalten unter Unsicherheit führt dazu, daß eher zu wenig Schutzmaßnahmen ergriffen werden.

2. Die Unter-(Über-)schätzung des Schadenpotentials risikoreicher wirtschaftlicher Aktivitäten aufgrund unzureichender Informationsversorgung führt zu einer ineffizient kleinen (großen) Nachfrage nach Sicherheitsvorkehrungen.

3. Bei exogen gegebenem Informationsdefizit der Nachfrager hinsichtlich der Effizienzeigenschaften der Sicherheitssysteme wird durch adverse Selektion und Moral Hazard der Markt für die guten Qualitäten nicht zustande kommen und deshalb ein volkswirtschaftlich suboptimales Sicherheitsniveau generieren.

---

[195] Da dies aber bei den meisten Verkehrssystemen der Fall ist, werden ihre Sicherheitseigenschaften von staatlichen Institutionen reguliert. Vgl. z. B. zur Flugsicherheit Rose (1992) oder zur Highway-Sicherheit Traynor & McCarthy (1991). In der Fallstudie werden in Abschnitt 2.6.3.2 die Interdependenzen zwischen den Sicherheitsrisken der Kommunikationssystemen und der Gesellschaft als Ganzes im Hinblick auf Externalitäten untersucht.

4. Endogenisiert man die Intensität der Informationsasymmetrie, indem man Screening- und Signaling-Strategien zuläßt, kommt es zwar zu einer Reduktion des Informationsdefizites, jedoch wird bedingt durch die Eigenschaften von Sicherheitssystemen und des Gutes Information nicht der volkswirtschaftlich effiziente Transparenzgrad erreicht, so daß dadurch wiederum zu wenig Schadensprävention betrieben wird.

5. Die von Sicherheitssystemen ausgelösten positiven Externalitäten sind die bedeutendste Quelle von Allokationsineffizienzen. Abgesehen von der Bereitstellung als reines Clubgut kommt es immer zu einem zu geringen Niveau an Sicherheitsmaßnahmen, wobei im Fall eines reinen öffentlichen Gutes die Diskrepanz zwischen realisierter und effizienter Allokation so groß ist, daß eine öffentliche Bereitstellung angemessen erscheint. Die Konstellation, in der das von Privaten genutzte Clubgut positive externe Effekte auf den Rest der Gesellschaft ausübt, macht u. U. auch eine direkte staatliche Intervention notwendig.

Die Darstellung verschiedener Lösungsmöglichkeiten, die geeignet sind, die dargestellten Allokationsineffizienzen auf den Märkten für Sicherheitsmaßnahmen zu vermeiden oder wenigstens zu reduzieren, wird Gegenstand des folgenden Kapitels sein.

1.5 Staatliche Instrumente zur Beseitigung der Allokationsineffizienzen auf Märkten für Sicherheitsgüter

1.5.1 Vorbemerkungen

Nachdem im vorangegangen Kapitel die wesentlichen nachfragebedingten Ursachen für Fehlallokationen auf den Märkten für Sicherheitsmaßnahmen identifiziert wurden, ist es das Ziel dieses Kapitels, fünf Instrumente darzustellen, welche in unterschiedlicher Weise dazu geeignet sind, die verschiedenen Allokationsineffizienzen abzubauen.[196] Es werden also nicht für jede Ursache von Ineffizienzen die entsprechenden Lösungsmöglichkeiten dargestellt, sondern es wird zunächst untersucht, auf welchen Marktmangel das jeweilige Instrumente angewandt werden kann, wobei jeweils verschiedene Ausgestaltungsmöglichkeiten aufgezeigt werden. Abschließend erfolgt eine Bewertung der verschiedenen Instrumente hinsichtlich der Kriterien Allokationseffizienz, Verteilungsgerechtigkeit und staatlicher Verwaltungsaufwand. Dieses allgemeinere Bewertungskonzept wurde von Calabresi (1970) angeregt, der bei der Untersuchungen über die Ausgestaltung über das Produkthaftungsrecht als Kriterien die Primary cost (= die Abweichung vom Allokationsoptimum), die Secondary cost (= Wohlfahrtsverluste durch eine ungleichmäßige Verteilung des anfallenden Schadens) und die Tertiary cost (= Verwaltungskosten) herangezogen hat.[197] Dabei wird eine Lösungsmöglichkeit einer anderen vorgezogen, wenn sie zur Realisierung eines Sicherheitsniveaus führt, welches dem optimalen näher kommt[198], wenn die Verteilung der Kosten für die zusätzlichen Präventionsmaßnahmen gleichmäßiger auf den Kreis der Betroffenen bei gleichzeitiger Einhaltung des Verursacher- bzw. Äquivalenzprinzips erfolgt und wenn die Kosten für den staatlichen Verwaltungsapparat - sei es die Justiz oder eine Regulierungsbehörde - geringer ausfallen.

Zunächst werden verschiedene Möglichkeiten der staatlichen Informationsbereitstellung vorgestellt, die zum einen die Unkenntnis der Nachfrager über ihre eige-

---

[196] Inwieweit sich Kombinationsmöglichkeiten verschiedener Instrumente zur Lösung anbieten wird in diesem Kapitel noch nicht dargestellt, sondern erfolgt erst in der Fallstudie bei der zusammenfassenden Bewertung der verschiedenen Instrumente in Abschnitt 2.7.7.

[197] Vgl. Calabresi (1970), S. 26ff, und Schäfer & Ott (1986), S. 85-92.

[198] Neben dem Kriterium, das nach Gleichung (19) bestimmte optimale Sicherheitsniveau s^* zu treffen, spielen bei der Bewertung der Instrumente noch ihre statische Effizienz, d. h. die Kostengünstigkeit hinsichtlich der Erreichung des vorgegebenen Ziels, und ihre dynamische Effizienz, d. h. ihre Eignung zusätzliche Innovations- und Vermeidungsanstrengungen anzuregen, eine entscheidende Rolle. Vgl. allgemein zu diesen Kriterien Fritsch, Wein und Ewers (1993), S. 66f.

nen Nachfragedeterminanten zu reduzieren vermögen und zum anderen die Informationsasymmetrien zwischen den Marktseiten abbauen helfen. Anschließend wird untersucht werden, inwieweit die zwei grundsätzlichen Formen des Haftungsrechtes, die Gefährdungs- und die Verschuldenshaftung, dazu beitragen können, die verschiedenen Quellen der Allokationsineffizienzen bei Sicherheitsmaßnahmen zumindest teilweise zu beheben. Zum dritten wird der Pigou-Vorschlag der auf den Preismechanismus gerichteten Steuer- und Subventionslösung dargestellt, der vor allem auf die Internalisierung der externen Effekte gerichtet ist. Nach der Abhandlung der marktkonformen Instrumente werden zwei ordnungsrechtliche Maßnahmen vorgestellt. Erst werden Eignung und Implikationen einer Regulierungslösung in Form von Mindestsicherheitsstandards untersucht. Anschließend wird die staatliche Bereitstellung von Sicherheitsmaßnahmen als direkteste Interventionsform des Staates vorgestellt und analysiert. Das Kapitel endet mit einer Übersicht über die Eignung der Instrumente bezüglich der Behebung der verschiedenen Allokationsineffizienzen und einer zusammenfassenden Bewertung, die auch die distributiven Konsequenzen und den anfallenden Verwaltungsaufwand miteinbezieht.

1.5.2 Staatliche Informationspolitik

1.5.2.1 Begründungen und Ziele

Aus dem vorangegangenen Kapitel ist hervorgegangen, weshalb die unzureichende Informationslage der Nachfrager nach Sicherheitsmaßnahmen zu einem ineffizienten Marktergebnis führen kann. Eine bessere und umfangreichere Informationsversorgung der Nachfrager schafft deshalb Abhilfe.

Da sich die staatliche Informationspolitik nicht zur Internalisierung externer Effekte eignet, weil den Wirtschaftssubjekten dadurch keine unmittelbaren Anreize, das volkswirtschaftlich effiziente Sicherheitsniveau anzustreben, geboten werden[199], kann sie potentiell auf zwei Quellen von Ineffizienzen einwirken. Zum einen kann das Verhalten der Individuen in der Weise beeinflußt werden, daß die Nutzenunkenntnis verringert wird, indem sowohl die Schadenpotentiale von wirtschaftlichen Aktivitäten bzw. von Produkten als auch die Effizienz von Sicherheitsmaßnahmen

---

[199] Vgl. zur Ineffizienz der Verbesserung des Umweltbewußtseins hinsichtlich direkter umweltfreundlicher Verhaltensänderungen Wicke (1993), S. 285f.

verdeutlicht werden.[200] Denn trotz der Marktmechanismen Signaling und Screening, die die ungleiche Informationskonstellation abbauen, werden durch eine bessere Informationsversorgung der weniger kundigen Wirtschaftssubjekte hinsichtlich der Determinanten ihrer Nachfrage nach Sicherheitsmaßnahmen Wohlfahrtssteigerungen erzeugt, weil eine Annäherung an das gesellschaftliche Allokationsoptimum ermöglicht wird. Zum anderen sind trotz guter Informationsversorgung unter Unsicherheit jedoch irrationale Verhaltensweisen zu beobachten, die durch eine inadäquate Informationsverarbeitung hervorgerufen werden.[201] Aufklärungspolitik kann dazu beitragen, daß die Individuen beim Vorliegen der wirklichen Nachfragedeterminanten eine ökonomisch rationalere Entscheidung über das Niveau an zu ergreifender Schadensprävention treffen. In der Realität sind beide Problembereiche jedoch nicht exakt zu trennen.

1.5.2.2 Ausgestaltungsformen

Bei der Darstellung der verschiedenen Formen der Informationspolitik wird zunächst kurz auf die Instrumente eingegangen, welche auf die Reduktion irrationaler Verhaltensweisen gerichtet sind, danach werden Möglichkeiten aufgezeigt, die nicht perfekten marktinternen Mechanismen Screening und Signaling zu verbessern.

Die auf der Irrationalität unter Unsicherheit fußenden Probleme bestehen - wie gezeigt - nicht in einer unzureichenden Informationsversorgung, sondern in der für die Erwartungsnutzenmaximierung inadäquaten Informationsverarbeitung. Deshalb muß bei den Nachfragern nach Sicherheitsmaßnahmen sowohl das Bewußtsein für Schadeneintrittswahrscheinlichkeiten und Schadenhöhen bzw. für Erwartungsschäden als auch ein Verständnis für das Erwartungsnutzenkonzept geschaffen werden. Schließlich müssen die daraus folgenden Konsequenzen für die Nachfrage nach Sicherheitsmaßnahmen abgeleitet werden.[202] Da Schäden oft nur im Zusammenhang mit der Anwendung eines bestimmten Produktes zur Ausübung einer Tätigkeit auftreten werden, sollte die Informationspolitik daran ansetzen, diese Schadenpo-

---

200 Hier geht es also vor allem darum, die Kenntnisse über die verschiedenen Nachfragedeterminanten zu verbessern.

201 Dies bedeutet, daß die Grenznutzenfunktion s^* von Gleichung (19) nicht nach dem Erwartungsnutzenkriterium abgeleitet wird. Vgl. dazu Abschnitt 1.4.2.

202 Letzteres ist besonders bei ökonomisch ungeschulten Verbrauchern erforderlich, wobei eine Verhaltensänderung durch die reine Übermittlung von Informationen nicht erreicht werden kann. Professionelle Nachfrager wie Unternehmen müssen dagegen auch unter Unsicherheit ökonomisch effiziente Entscheidungen treffen.

tentiale und die Möglichkeiten entsprechender Sicherheitsmaßnahmen beim Benutzer bewußt zu machen.

In Anbetracht der trotz marktimmanenter Mechanismen noch bestehenden Informationsasymmetrien muß die Informationspolitik in zwei verschiedenen Märkten ansetzen. Zunächst müssen die Verbraucher genauere Informationen über die Schadenpotentiale ihrer wirtschaftlichen Aktivitäten bzw. ihrer benutzten Produkte erhalten, damit die antizipierten Schadenswahrscheinlichkeiten und Schadenhöhen nicht mehr von den wahren abweichen. Zusätzlich muß auf den Märkten für Sicherheitsmaßnahmen die Qualität der Informationen über die Wirksamkeit der Sicherheitssysteme verbessert werden, damit die individuelle Einschätzung hinsichtlich deren Effizienz berichtigt werden kann. Da es sich in beiden Fällen um qualitativ gleiche Lösungsansätze handelt, wird - soweit keine wesentlichen Unterschiede existieren - nicht zwischen Informationspolitik auf den Märkten risikobehafteter Produkte und von Sicherheitssystemen differenziert.

Prinzipiell setzt Informationspolitik[203] an der Unterstützung der Informationsasymmetrien abbauenden Mechanismen an. So kann Screening[204] kostengünstiger und effizienter gestaltet werden, indem Informationsbeschränkungen von seiten der Anbieter reduziert werden, ein gewisses Maß an Informationsbereitstellung obligatorisch wird und vergleichende Gütertests durchgeführt werden.[205] Schließlich kann die Arbeit von Spezialisten - wie der Verbraucherverbände oder der Stiftung Warentest[206] - durch die Subventionierung der Informationsbeschaffung und -verbreitung gefördert werden, so daß diese Informationsinhalte kostengünstig an die Verbraucher weitergegeben werden können.[207]

---

203 Informationspolitik beinhaltet zwar auch regulative Elemente und finanzielle Anreize, aber durch die Konzentration auf die Informationsproblematik kann sie als eigenständiges Politikinstrument angesehen werden. Vgl. dazu auch die Unterscheidung von Shapiro (1983), S. 528f.

204 Vgl. zu den Informationsstrategien u. a. Vahrenkamp (1991), S. 114-132, und Beales, Craswell und Salop (1981), S. 514-526.

205 Dies bedeutet in unserem Kontext, daß das Ausmaß der Schadenpotentiale und die nach Ergreifung von Sicherheitsmaßnahmen verbleibenden Restrisiken nicht verschwiegen werden dürfen, sondern die Verbraucher darüber explizit informiert werden müssen.

206 Zusammenstellungen der verschiedenen Verbraucherorganisationen in Deutschland sind in Schöppe (1983), S. 550f, und in Kuhlmann (1990), S. 420-426, zu finden.

207 Vgl. dazu Vahrenkamp (1991), S. 133-153. Neben der Kostensenkung im Bereich des Signaling hält Cooper (1992), S. 433, auch die Kostenerhöhung im Fall falscher Signale für ein geeignetes Instrument zum Abbau von Informationsasymmetrien.

Das Signaling kann vor allem mittels der Beeinflussung des Reputationsmechanismus an Effektivität gewinnen.[208] Die Motivation zur Reputationsbildung ist eher gering, wenn die Verbraucher ihre Qualitätserwartungen nur unvollständig und langsam aktualisieren.[209] So offenbart sich das wichtige Qualitätsattribut Sicherheit bzw. Schadenanfälligkeit meist erst nach einem längeren Nutzungszeitraum oder schlechte Leistungen werden als Ausreißer und nicht als konstitutive Qualitätseigenschaft interpretiert. Schließlich sind die Gewinnmöglichkeiten aus verdeckter Qualitätsverschlechterung beträchtlich, wenn die einzelnen Produkte nicht den jeweiligen Anbietern zugeordnet werden.

Deshalb müssen die Bildung korrekter Qualitätserwartungen der Konsumenten und deren schnelle Verbreitung beeinflußt werden, indem folgende informationspolitische Maßnahmen ergriffen werden.[210] Es können allgemeine Produktkenntnisse zur kritischen Begutachtung der Qualität vermittelt werden. Die Bereitstellung komplementärer Qualitätsinformationen vermag die Einordnung subjektiver Erfahrungen zu verbessern. Die Veröffentlichung von aggregierten negativen Schadensinformationen erleichtert die Bestimmung von durchschnittlichen Schadeneintrittswahrscheinlichkeiten und -höhen und der Effizienz von Sicherheitsmaßnahmen.[211] Schließlich begünstigt die Produktkennzeichnung die Identifikation von Produkten. Eine Reduktion der Gewinnmöglichkeiten aus verdeckten Qualitätsverschlechterungen kann im Rahmen der Informationspolitik durch das Verbot irreführender Werbung erreicht werden. Die Glaubwürdigkeit der Anbieter steigt auch durch die Untersagung bzw. Sanktionierung irreführender Informationen.[212] Bei langlebigen Gütern spielt - wie in Abschnitt 1.4.4 gezeigt wurde - die Garantiegewährung eine große Rolle. Die Informationspolitik kann in diesem Fall durch die Standardisierung und Vereinfachung der Garantieklauseln die Aufnahme von Qualitätssignalen erleichtern und damit die Allokation verbessern.[213]

---

208 Vgl. dazu Vahrenkamp (1991), S. 51.

209 Shapiro (1983), S. 675, zeigt, daß die Wohlfahrtsverluste um so größer sind, je langsamer die Konsumenten die Produkteigenschaften kennenlernen.

210 Vgl. dazu Vahrenkamp (1991), S. 52f.

211 Maßnahmen, die die Effektivität des Signaling erhöhen, überschneiden sich z. T. mit Screening erleichternden Strategien.

212 Hierunter kann z. B. verstanden werden, daß Fehlerwahrscheinlichkeiten und Schadenhöhen positiv ausgedrückt bzw. die nach der Ergreifung von Sicherheitsmaßnahmen bleibenden Schadenpotentiale angegeben werden müssen.

213 Vgl. dazu Cooper (1992). Eine weitere Möglichkeit der Schaffung von Qualitätssignalen ist die staatliche Zertifizierung, wie es der europäische Qualitätsstandard ISO 9000 vorsieht. Vgl. dazu Vahrenkamp (1991), S. 69.

1.5.2.3 Bewertung

Nach der knappen Aufzählung verschiedener Möglichkeiten einer staatlichen Informationspolitik wird eine Bewertung dieser Strategie hinsichtlich verschiedener Kriterien vorgenommen. Zunächst soll ihre Effektivität bezüglich der Beseitigung der durch Irrationalitäten und Informationsasymmetrien hervorgerufenen Allokationsineffizienzen untersucht werden.

Da es sich bei irrationalen Entscheidungen nicht um Informationsprobleme handelt, ist Informationspolitik weniger geeignet, weil sie eigentlich nicht auf die Informationsverarbeitung und die Entscheidungsfindung der Wirtschaftssubjekte abzielt. Wirkungsvoller ist ihr allokativer Effekt hinsichtlich asymmetrischer Informationsverteilung zu bewerten. Im allgemeinen berührt Informationspolitik die Konsumentensouveränität nicht, weil die Anbieter unbeschränkt auf die unbeeinflußten Präferenzen bzw. auf den individuellen Trade off zwischen Preis und Qualität reagieren können.[214] Die Effektivität der Informationspolitik hängt jedoch davon ab, inwieweit die informierten Konsumenten ihre Qualitätsvorstellungen durchzusetzen vermögen.[215] Dies bedeutet, daß Informationspolitik besonders auf den Märkten seine Wirksamkeit entfalten wird, wo bereits die Marktmechanismen des Signaling und des Screening dafür sorgen, daß Informationsasymmetrien abgebaut werden. Schließlich sind zwar die Wohlfahrtsverluste aufgrund von Fehleinschätzungen der staatlichen Instanzen eher gering einzuschätzen, jedoch ist das erfolgreiche Eingreifen in den Informationsmarkt unwahrscheinlicher als die obligatorische Vorgabe von Sicherheitsstandards für risikoreiche Produkte, so daß mit dem Instrument der Informationspolitik zwar relativ wenig falsch gemacht werden kann[216], aber schnelle und merkliche Allokationsverbesserungen nicht erwartet werden können.

Differenziert man die Allokationseffizienz der Informationspolitik bezüglich der beiden Informationsstrategien Screening und Signaling, kommt man zunächst bezüglich Screening zu folgendem Ergebnis. Das Ausmaß asymmetrischer Information und damit des Marktversagens hängt von der Höhe der Informationskosten ab.

---

[214] Vgl. dazu Beales, Craswell und Salop (1981), S. 513f.

[215] Dies hängt vor allem von der Wettbewerbs- bzw. Angebotssituation ab. So werden sich die Sicherheitspräferenzen der Nachfrager in einem Markt mit starkem Wettbewerbsdruck im Vergleich zu einem monopolisierten Markt leichter durchsetzen lassen.

[216] Es können negative Rückwirkungen eintreten, wenn z. B. die Überbewertung von Risiken zu einer allgemeinen Skepsis unter den Konsumenten führt und damit die Einführung von Innovationen verhindert. Umgekehrt können unterbliebene Warnungen zu Katastrophen mit irreparablen Schäden führen. Vgl. dazu Foster & Just (1989), die Wohlfahrtseffekte unterschiedlicher Informationsstrategien im Falle von Lebensmittelverunreinigungen untersuchen.

Erreichen diese eine gewisse Höhe, sinkt dadurch die zusätzliche aggregierte Zahlungsbereitschaft der Nachfrager für höhere Qualitätsniveaus so stark ab, daß sich für die Anbieter eine verdeckte Qualitätsverschlechterung lohnt und langfristig durch diese adverse Selektion nur niedrige Produktqualitäten angeboten werden. Durch die kostenlose bzw. -günstige Bereitstellung sinken die Informationskosten für die Nachfrager, und die Anbieter haben nun wieder einen stärkeren Anreiz, bessere und sicherere Produkte zu produzieren. Ist die Erzeugung und Verbreitung der Informationen nicht übermäßig kostenintensiv, dann ist eine solche Politik wohlfahrtssteigernd.[217] Bei Sicherheitsmaßnahmen - vor allem im Zusammenhang mit komplexen technischen Systemen - kann der Aufwand zur Bestimmung des exakten Schadenpotentials und besonders der Effektivität von Sicherheitssystemen u. U. so umfangreich sein, daß die Maßnahmen staatlicher Informationspolitik keine Wohlfahrtssteigerungen hervorbringen.

Da die Anbieter bezüglich ihrer Produkte einen Informationsvorsprung haben, können sie zusätzlich zu ihren freiwilligen Signalingaktivitäten auch den gesetzlichen Offenlegungs- und Informationspflichten relativ kostengünstig gerecht werden.[218] Falls der drohende Verlust von Wiederholungskäufen[219], der den Anbieter zum Einhalten der versprochenen Qualität zwingt, durch die Langlebigkeit der mit Risikopotentialen behafteten Basisprodukte oder der Sicherheitsgüter nicht funktioniert, erscheint die Unterstützung der Garantiegewährung, eine Erleichterung des Signaling vorteilhaft, weil es zum einen durch seine Flexibilität allokationseffizienter und zum anderen kostengünstiger ist.[220] Jedoch können, falls nur wahre Informationen veröffentlicht werden, durch Offenlegungsverpflichtungen auch negative Wohlfahrtseffekte entstehen, weil dann die Signaling-Anreize so stark sind, daß eine Besteuerung der Veröffentlichung von Produktinformationen vorteilhafter ist.[221]

Faßt man die Allokationseffizienz der Informationspolitik in bezug auf die beiden Instrumente zusammen, kann nur festgestellt werden, daß die Informationspolitik im Fall von Sicherheitssystemen stärker die Screening-Strategien unterstützen sollte. Denn Signaling in Form von Reputationsstrategien und von Garantiegewährung ist eher für kurzlebige Produkte, deren Qualitätseigenschaften leicht zutage

217 Vgl. dazu Vahrenkamp (1991), S. 159.
218 Vgl. dazu u. a. Magoulas (1985), S. 42.
219 Vgl. dazu Klein & Leffler (1981), S. 616.
220 Vgl. dazu Cooper (1992), S. 447f.
221 Vgl. dazu Jovanovic (1982), S. 41ff.

treten, geeignet. Aber sowohl Sicherheitsgüter als auch Produkte mit großem Schadenpotential werden von den Nachfragern meist nur selten oder gar einmalig angeschafft. Außerdem sind die Eigenschaften von Sicherheitssystemen für eine Garantiegewährung eher ungeeignet.[222]

Bezüglich der Verteilungsaspekte kann man folgende Unterscheidung treffen. Werden die Anbieter zu einer umfangreicheren Informationsbereitstellung verpflichtet, versuchen sie die dadurch anfallenden Kosten gleichmäßig auf die Nachfrager zu überwälzen. So werden letztendlich unter Vernachlässigung von Externalitäten gemäß dem Äquivalenzprinzip die Kosten der staatlichen Informationspolitik von den Nutznießern, den Benutzern von risikobehafteten Produkten und den Nachfragern nach Sicherheitsgütern getragen.[223] Im Gegensatz dazu werden der Gesellschaft bzw. der Gemeinschaft der Steuerzahler die Kosten der Informationspolitik aufgebürdet, wenn entweder staatliche Stellen - wie Prüfungsinstitutionen - die Produktinformationen kostenlos den betroffenen Nachfragern zur Verfügung stellen oder die private Informationsbeschaffung und Produktprüfung subventioniert werden. In diesem Fall ist das Äquivalenzprinzip nicht erfüllt, außer wenn durch den Abbau der Informationsasymmetrien auch existierende negative Externalitäten reduziert werden.

Schließlich kann konstatiert werden, daß Informationspolitik im allgemeinen bezüglich des staatlichen administrativen Aufwandes als günstig anzusehen ist, wobei die Erlassung von Informationspflichten nur die Kosten der Überprüfung bezüglich der Einhaltung in Einzelfällen nach sich ziehen, während bei der Unterstützung privater Informationsanbieter mittels Subventionen genauso wie bei der staatlichen Informationsbereitstellung durch eine eigenständige Institution permanent Kosten anfallen.[224]

---

[222] Vgl. dazu Abschnitt 1.4.4.

[223] Differenziert man die Gruppe der Nachfrager nach risikobehafteten Gütern, werden diejenigen durch die Erlassung von Informationspflichten besonders belastet, welche gegenüber den bestehenden Schadenpotentialen indifferent sind und deshalb auch keine sichereren Produkte nachfragen.

[224] Es stellt sich zwar noch zusätzlich die Frage, ob die staatliche Informationsbeschaffung kostengünstiger ausfällt als die Zuteilung von Subventionen an private geprüfte Informationsanbieter, aber dies ist nicht Gegenstand der Untersuchung.

1.5.3 Haftungssysteme

1.5.3.1 Begründungen und Ziele

Wie im vorangegangenen Abschnitt dargestellt, wird mit Hilfe der Informationspolitik versucht ex ante auf die Allokationsineffizienzen einzuwirken. Rechtsvorschriften dagegen regeln und beeinflussen das Zusammenleben der Wirtschaftssubjekte nach Eintreten eines Konflikt- oder Schadenfalls.[225] Das Haftungsrecht wird also erst ex post wirksam, indem es die entstandenen Schäden[226] auf bestimmte Individuen - Verursacher oder Geschädigte - zu verteilen versucht. Durch die Zuordnung der durch Handlungsfolgen von wirtschaftlichen Aktivitäten anfallenden Kosten stellen Haftungsregeln gleichzeitig Nebenbedingungen dar, welche eine Zielfunktion, wie die individuelle Erwartungsnutzenmaximierung, beschränken und damit auch eine Allokationsfunktion haben, indem sie wie ein impliziter Preis für die Verursachung eines Schadenfalls wirken und damit Anreize zur Schadenverhütung erzeugen.

Die Allokationswirkung von Haftungsregeln kann wie folgt beschrieben werden. Sie haben den Charakter einer Internalisierungsstrategie, indem das Ergebnis der individuellen Gewinn- und Nutzenmaximierung, welches durch die Ausübung verschiedener Tätigkeiten Schadensrisiken mitsichbringt, mit dem volkswirtschaftlichen Optimum in Übereinstimmung gebracht wird.[227] Dies wird durch die nachträgliche Sanktionierung von Vertrags- und Eigentumsverletzungen, über die ex ante nicht verhandelt wurde, bewerkstelligt. So soll Einfluß auf die Erwartungsbildung potentieller Schädiger und Geschädigter genommen werden, damit diese die durch Produktunfälle und unerlaubte Handlungen entstehenden Schäden - unter Berücksichtigung der anfallenden Vermeidungskosten - zu minimieren suchen. Zwar setzen die Folgen der Haftung erst ex post nach dem Schadenseintritt ein, aber dieses Ausmaß hängt von der ex ante Initiative der Privaten - d h. von ihren

---

[225] Vgl. dazu Koboldt, Leder und Schmidtchen (1992), S. 334, und ebenda zu einem Überblick über die ökonomische Analyse des Rechts, die in ihren Basismodellen perfekte Informiertheit aller beteiligten Akteure über Erwartungsschäden, Sicherheitsvorkehrungen, geforderte Sorgfaltsstandards, Kausalitäten und Identität von Schaden und Schadenskompensation unterstellt. Falls keine speziellen Einschränkungen gemacht werden, wird vor dem Hintergrund dieser Annahmen argumentiert.

[226] Auf die Bewertungsproblematik, welche besonders bei immateriellen Schäden auftaucht, wird in diesem Abschnitt nicht eingegangen. Es wird deshalb auf Abschnitt 2.5.2 der Fallstudie und auf Endres (1991), S. 54f, Schäfer & Ott (1986), S. 179-185, S. 227-240, und Adams (1989), S. 210-217, verwiesen.

[227] Vgl. Endres (1991), S. 2f.

Schadenvermeidungsaktivitäten bzw. von ihren getroffenen Sicherheitsmaßnahmen - ab. Es stellt sich nun die Frage, inwieweit das Haftungsrecht die Behebung der durch Irrationalitäten, Informationsasymmetrien und Externalitäten verursachten Allokationsineffizienzen zu unterstützen vermag.

Kategorien des Haftungsrechts / Eigenschaften	Produzentenhaftung	Haftungsrecht im Sinne des Rechts unerlaubter Handlungen
Verursacher	Anbieter risikoreicher Produkte	Betreiber risikoreicher Anlagen und Aktivitäten
Opfer	Nachfrager risikoreicher Produkte	Unfallopfer, die in keinem vertraglichen Verhältnis zum Verursacher stehen
Ziele	Vermeidung irrationalen Nachfragerverhaltens Abbau asymmetrischer Informationsverteilung	Internalisierung negativer Externalitäten

Übersicht 2: Produzentenhaftung versus Haftungsrecht im Sinne des Rechts unerlaubter Handlungen

Während sich die Informationspolitik auf die Beseitigung von Informationsasymmetrien auf den Märkten von risikobehafteten Produkten und von Sicherheitsmaßnahmen konzentriert, kann das Haftungsrecht seine Wirkung vor allem im Bereich der Produktsicherheit und -verwendung entfalten. Dies bedeutet zum einen, daß die Anbieter von Produkten mit Sicherheitsrisiken aufgrund der Produkt- bzw. Produzentenhaftung[228] Sicherheitsvorkehrungen bereits bei der Planung berücksichtigen und diese deshalb in die Produktausstattung integrieren. Die Entscheidung über das Ausmaß der zu ergreifenden Sicherheitsmaßnahmen wird deshalb zum größten Teil von den Produzenten getroffen. Nur bezüglich des verbleibenden Restrisikos bleibt den einzelnen Konsumenten die Möglichkeit, zusätzliche Nachfrage nach Sicherheitsgütern zu entfalten. Zum anderen können die Wirtschaftssubjekte hinsichtlich der externen Effekte von Präventionsmaßnahmen durch die Regeln des Rechtes

[228] Vgl. zur Differenzierung der beiden Begriffe Wischermann (1991), S. 2f. In der weiteren Darstellung werden die Ausdrücke synonym verwendet.

unerlaubter Handlungen dazu gebracht werden, die bei anderen Individuen anfallenden Schäden in ihre Erwartungsnutzenfunktion zu integrieren. Übersicht 2 auf der vorangegangenen Seite macht vorab deutlich, welche Allokationsineffizienzen durch die verschiedenen Kategorien des Haftungsrechts abgebaut werden können.

Das irrationale Verhalten unter Unsicherheit hat - wie in Abschnitt 1.4.2 gezeigt - seine Ursache in der inadäquaten Verarbeitung der gegebenen Informationen über die relevanten Parameter und führt durch die Unterschätzung des Nutzenverlustes im Schadensfall gemeinhin zu suboptimalen Sicherheitsmaßnahmen. Die Regeln des Haftungsrechtes sollen die so ausgelösten Ineffizienzen beseitigen bzw. eindämmen, indem den Akteuren, die unter Unsicherheit zu rationalen Entscheidungen fähig sind, die Verantwortung bezüglich der Entscheidung über das zu ergreifende Sicherheitsniveau zugeschrieben und dadurch eine effizientere Allokation erreicht wird. Dies ist gemeinhin die Anbieterseite, weil ineffizient entscheidende Anbieter aufgrund des Wettbewerbdruckes langfristig aus dem Markt verdrängt werden.

Ähnlich wie zur Verhinderung irrationalen Verhaltens unter Unsicherheit kann das Haftungsrecht auch - zumindest indirekt - zum Abbau von Informationsasymmetrien beitragen, indem den unzureichend informierten Marktteilnehmern die Verantwortung für ihre Aktivitäten teilweise oder ganz abgenommen wird und entsprechend die besser informierte Marktseite - wiederum die Anbieter - die Handlungsfolgen zu tragen hat. Sie hat deshalb einen Anreiz, bis zu dem Grad Sicherheitsmaßnahmen in die Produkte zu integrieren, welcher ihr einen maximalen Gewinn einbringt und der Gesellschaft ein höheres Wohlfahrtsniveau. Über den Marktpreis, der c. p. um so höher ist, je mehr Sicherheitsvorkehrungen in das Produkt eingebaut werden, findet damit ein indirekter Abbau der Informationsasymmetrien statt.[229]

Schließlich hat das Haftungsrecht und die Schadenersatzpflicht bei unerlaubten Handlungen wesentliche theoretische und auch praktische Bedeutung bei der Internalisierung externer Effekte - vor allem im Bereich der Umweltschäden - erlangt.[230] Denn nach Coase (1960) können externe Effekte durch die exakte Bestimmung von Eigentumsrechten internalisiert werden. In diesem hier vorliegenden

---

229 Vgl. dazu auch Spence (1977), S. 569.

230 Damit können nicht die positiven, sondern nur die negativen, durch Unfälle verursachten Externalitäten von Sicherheitsmaßnahmen internalisiert werden. Vgl. in der Bundesrepublik dazu das Produkthaftungsgesetz (ProdHaftG) im BGBl. S. 2198 vom 15. 12. 1989 und §823 BGB.

Zusammenhang wird untersucht, inwieweit Externalitäten, die durch die Ergreifung bzw. Unterlassung von Sicherheitsmaßnahmen hervorgerufen werden, durch eine entsprechende Ausgestaltung des Haftungsrechtes internalisiert werden können und dadurch die Allokationseffizienz auf dem Markt für Sicherheitsgüter und -vorkehrungen erhöht werden kann.[231]

1.5.3.2 Ausgestaltungsmöglichkeiten des Haftungsrechtes

Es werden die in der Literatur am häufigsten analysierten und in der Rechtspraxis vorherrschenden Haftungssysteme - die Verschuldens- und die Gefährdungshaftung - und ihre Wirkungen auf die genannten Ansatzpunkte dargestellt, wobei zur Veranschaulichung der Effizienz im Falle von irrationalem Verhalten und von Informationsasymmetrien bei Bedarf als Vergleichsbasis die reine Konsumentenhaftung herangezogen wird.[232]

Die Darstellung und die Analyse der Wirkungsweise der beiden Haftungsregeln geht wiederum von der in Kapitel 1.2 nach dem Erwartungsnutzenkonzept abgeleiteten Grenznutzenfunktion von Sicherheitsgütern und -maßnahmen s* aus. Bezüglich des irrationalen Verhaltens der Wirtschaftssubjekte und der bestehenden Informationsasymmetrien stellt sich die Frage, ob im Vergleich zur bisher implizit unterstellten Konsumentenhaftung[233] die Verschuldens- und die Gefährdungshaftung als Formen der Produzentenhaftung eine Verbesserung der Allokation bewirken können. Im Gegensatz dazu steht bezüglich der Externalitäten generell zur Diskussion, ob die Gefährdungs- oder die Verschuldenshaftung des allgemeinen Deliktrechtes besser zur Erreichung des gesamtwirtschaftlichen Optimums geeignet ist.[234] Bevor die Allokationseffekte der beiden Haftungssysteme bezüglich der ver-

---

231 Vgl. dazu auch Endres (1991), S. 29-33. Bei einer weitreichenden Produkthaftung, muß der Produzent auch für Schäden der Produktverwendung aufkommen, die nicht nur dem Anwender, sondern auch Dritten entstehen. Auf diesem indirekten Wege kann auch die Produzentenhaftung auch zu einer Internalisierung externer Effekte führen. Vgl. zu dieser Strategie den Vorschlag eines Informationssicherheitshaftungsgesetzes in Abschnitt 2.7.3.5 der Fallstudie.

232 In den frühen ökonomischen Auseinandersetzungen bzgl. des Haftungsrechtes stand die Diskussion um die Vorteilhaftigkeit der Konsumenten- (caveat emptor) vs. der Produzentenhaftung (caveat venditor) im Vordergrund. Vgl. dazu die Reihe von Beiträgen in The University of Chicago Law Review 38/1970 von u. a McKean und Buchanan.

233 Unter diesem Haftungsregime müssen die Konsumenten für alle Schäden aufkommen, die durch ihre wirtschaftlichen Aktivitäten - also auch durch den Gebrauch von Schäden verursachenden Produkten - eintreten können.

234 Eine Unterteilung der Wirtschaftssubjekte in Produzenten und Konsumenten ist bei der Internalisierung von durch Sicherheitsmaßnahmen ausgelösten Externalitäten nicht sinnvoll, denn hier geht

schiedenen Problemfelder bestimmt werden können, bedarf es zunächst genauer Definitionen der beiden Begriffe.[235]

Gefährdungshaftung

Bei der Gefährdungshaftung hat das Wirtschaftssubjekt - Produzent oder allgemein Schadenverursacher - unabhängig davon, wieviel Sorgfalt bzw. Vorsichtsmaßnahmen es getroffen hat, für alle durch seine Aktivitäten ausgelösten Schäden aufzukommen.[236] Es ist die weitreichendste Haftungsregel, und es muß nicht geklärt werden, ob durch fahrlässiges oder vorsätzliches Verhalten Verschulden vorliegt oder nicht.

Verschuldenshaftung

Im Rahmen der Verschuldenshaftung kann sich der Verursacher durch sorgfältiges und nicht vorsätzliches Verhalten von der Kompensationspflicht der entstehenden Schäden befreien. Unter Vernachlässigung von Informationsproblemen ist es ökonomisch effizient, den geforderten Sorgfaltsstandard jeweils auf das aus einer rationalen, alle Schadenkomponenten berücksichtigenden Erwartungsnutzenmaximierung abgeleitete Sicherheitsniveau s^* festzulegen.

Bei rationalen und wohlinformierten Nachfragern, die den gleichen Erwartungsschaden haben und risikoneutral sind, führen sowohl Verschuldens- als auch Gefährdungshaftung dazu, daß die Produzenten das gesamtwirtschaftlich effiziente Ausmaß an Sicherheitsvorkehrungen in ihre Produkte installieren.[237] Dies bedeutet, daß die Anbieter die optimale Mischung aus Aufwendungen für in die Produkte installierten Sicherheitssysteme und für Haftpflichtversicherungen[238] auswählen und damit die Konsumenten keine Entscheidung mehr über das individuelle Präventionsniveau treffen müssen. Unterstellt man dagegen bezüglich Schadenpotential und Risikoaversion heterogene Nachfrager, dann führt die Verschuldenshaftung dazu, daß der Produzent der geforderten Sorgfaltspflicht durch den Einbau von Si-

---

es nicht um Produkthaftung, sondern generell um das Schadensrecht bei Unfällen zwischen Fremden, die keine vertragliche Beziehung verbindet.

235 Vgl. dazu und weiteren Haftungssystemen wie der Mitverschuldensklausel Endres (1991), S. 6f, und die kurze Übersicht von Koboldt, Leder und Schmidtchen (1992), S. 38ff, und Cooter (1991) oder speziell zur Umwelthaftung Cansier (1993), S. 242-280.

236 Nach Shapiro (1991), S. 6, ist die Gefährdungshaftung ein Spezialfall der Verschuldenshaftung, welche einen so hohen Sorgfaltsstandard fordert, daß kein potentieller Verletzer diesen erreichen kann.

237 Vgl. dazu u.a. Adams (1987), S. 8.

238 Die Haftpflichtversicherung ist sowohl Substitut als auch Komplement zu Sicherheitsvorkehrungen. Vgl. zur Produkthaftung und Versicherung Adams (1987), S. 16ff, und zu Haftung und Versicherung Endres (1991), Kapitel D.

cherheitsvorkehrungen gerecht wird und die Wirtschaftssubjekte die Möglichkeit haben, weitere Sicherheitsvorkehrungen zu treffen, bis sie das für sie individuell optimale Niveau erreichen und damit eine effiziente Allokation herbeiführen. Hingegen kommt es unter der Gefährdungshaftung zu einer Subventionierung der Kunden mit hohem Schadenpotential durch diejenigen mit geringen Erwartungsschäden, weil der Anbieter die Nachfrager nicht nach ihrem Schadenpotential differenzieren kann. Deshalb muß er bei der Installation von Sicherheitsmaßnahmen und bei der Absicherung durch eine Haftpflichtversicherung von einem durchschnittlichen Erwartungsschadens ausgehen. Dies wird sich in einem höheren Produktpreis als unter Verschuldenshaftung niederschlagen.[239] Durch die Gefährdungshaftung wird für die meisten Wirtschaftssubjekte eine eigene Entscheidung hinsichtlich zu ergreifender Sicherheitsvorkehrungen hinfällig. Nur diejenigen, welche trotz materieller Kompensation durch einen Schadensfall immer noch Wohlfahrtsverluste erleiden, werden zusätzlich individuelle Sicherheitsmaßnahmen vornehmen. Jedoch können langfristig durch den Prozeß der adversen Selektion, welcher die Kunden mit geringen Schadenpotentialen aus der Gesamtnachfrage ausscheiden läßt, und Moral Hazard weitere Fehlallokationen ausgelöst werden.[240]

Neben den verschiedenen Haftungsregeln, die zwischen Anbietern und Nachfragern gelten, muß auch noch die Schadensfallkonstellation betrachtet werden, wo zwischen dem Schadenverursacher und den betroffenen Opfern keine vertraglichen Beziehung bestehen. Unter Gefährdungshaftung hat der Verursacher in jedem Fall die gesamten Schäden aller Dritten ohne Berücksichtigung deren Verhalten zu kompensieren. Unterstellt man eine vollständige Wiederherstellung des ursprünglichen Zustandes, haben die potentiellen Opfer keinen Anreiz, Sicherheitsvorkehrungen zu treffen. Haftet der Verursacher jedoch nur dann, wenn er fahrlässig oder vorsätzlich den Schadensfall herbeigeführt hat, dann ist davon auszugehen, daß er Sicherheitsvorkehrungen in dem Ausmaß ergreift, das ihn von der Haftung befreit. Damit ist aber unmittelbar verbunden, daß bei den dann noch anfallenden Schadensfällen die Opfer ihre Schäden selbst zu tragen haben. Sie haben deshalb in diesem Fall einen Beweggrund, sich gegen das Restrisiko, falls überhaupt möglich, mit angemessenen Sicherheitsmaßnahmen zu schützen.[241]

---

239 Weitere Aspekte, welche die Effizienz eines Haftungssystems beeinflussen, sind die Marktstruktur und die Versicherungsmöglichkeit der Risiken. Vgl. dazu Epple & Raviv (1978).

240 Vgl. dazu Adams (1987) S. 6f.

241 In der weiteren Untersuchung wird die Einflußmöglichkeit der Konsumenten bzw. Opfer auf die Schadenswahrscheinlichkeit und -höhe ausgeschlossen, weil dies auch für die Situation der Informationssicherheit in Kommunikationssystemen angebracht ist.

1.5.3.4 Bewertung der Haftungssysteme

Nach der Darstellung der Wirkungsweise der Haftungssysteme ohne Berücksichtigung der nachfragebedingten Allokationsineffizienzen, wird nun eine vergleichende Bewertung hinsichtlich ihrer Eignung zur Behebung dieser Mängel, ihrer Verteilungskonsequenzen und des auf Grund der Haftungssysteme laufend entstehenden staatlichen Verwaltungsaufwandes durchgeführt.

Unterstellt man nun den realistischen Fall, daß die Nachfrager aufgrund von Informationsasymmetrien und Entscheidungsanomalien das Risiko unterschätzen und der Produzent unter der Verschuldenshaftung das geforderte Sorgfaltsniveau einhält, dann werden sie wiederum zu geringe Sicherheitsmaßnahmen unternehmen - wenngleich relativ zur reinen Konsumentenhaftung eine Allokationsverbesserung durch die vom Produzenten unternommenen Sicherheitsmaßnahmen eintritt. Die Gefährdungshaftung sorgt jedoch in einer solchen Konstellation dafür, daß sich in den höheren Produktpreisen das gesteigerte Schadenpotential genau widerspiegelt, weil die Produzenten sowohl höhere Prämien an die Haftpflichtversicherung entrichten müssen als auch verstärkt Sicherheitsmaßnahmen in die Produkte integrieren werden.[242] Bei der Gefährdungshaftung wird die Entscheidung über das Sicherheitsniveau im Gegensatz zur Verschuldenshaftung vollständig von den Anbietern getroffen, so daß die durch irrationale und uninformierte Nachfragerentscheidungen ausgelösten Allokationsineffizienzen beseitigt werden.[243] Jedoch bleiben die durch die Heterogenität und Nichtidentifizierbarkeit des Risikos der verschiedenen Konsumententypen hervorgerufenen statischen und dynamischen Ineffizienzen.

Auch im Falle von Externalitäten der Sicherheitsvorkehrungen werden die beiden Alternativen Gefährdungs- und Verschuldenshaftung darauf untersucht, inwieweit sie geeignet sind, das gesellschaftliche optimale Ausmaß an Sicherheitsmaßnahmen zu erreichen.[244] Das Kriterium der statischen Allokationseffizienz, welches fordert, daß jedes Wirtschaftssubjekt das gemäß seiner individuellen Parameter optimale Sicherheits- oder Sorgfaltsniveau verwirklicht, erfüllt die Gefährdungshaftung durch eine nach dem Erwartungsnutzenkriterium abgeleitete und auch realisierte

---

[242] Es wird angenommen, daß die Anbieter die Risiken korrekt einschätzen können. Vgl. zur Risikofehlwahrnehmung der Produzenten Adams (1987), S. 14f.

[243] Allerdings konnten Untersuchungen in den Vereinigten Staaten nicht belegen, daß der Übergang von der Verschuldenshaftung auf die Gefährdungshaftung zu einem Rückgang der Unfallhäufigkeit führt. Vgl. dazu die Quellen in Priest (1991), S. 42ff.

[244] Vgl. dazu und dem folgenden Fritsch, Wein und Ewers (1993), S. 96-99.

Nachfrage nach Sicherheitsgütern und -maßnahmen auf jeden Fall.[245] Die Verschuldenshaftung wird dieser Anforderung nur unter der Annahme homogener Verursacher gerecht, weil nur dann das in der Rechtspraxis durchschnittliche geforderte Sorgfaltsniveau[246] dasselbe ist wie das aufgrund der Gefährdungshaftung freiwillig realisierte. Da aber innerhalb einer Gruppe gleichartiger potentieller Verursacher - Ärzte, Autofahrer, etc. - erhebliche Unterschiede in den einzelnen Parametern - wie Erwartungsschaden und Effektivität der Sicherheitsvorkehrungen - bestehen, wird ein einheitlicher Vorsorgemaßstab sowohl zu über- als auch zu unteroptimalen Sicherheitsmaßnahmen führen und damit das statische Effizienzkriterium nicht erfüllen.[247]

Neben der statischen Allokationseffizienz haben die beiden Haftungsregime auch Einfluß auf die Anstrengungen, neue kostengünstige Sicherheitssysteme zu entwikkeln und Informationen über den potentiellen Schadenumfang zu beschaffen.[248] Unter der Verschuldenshaftung kann der Verursacher nur Kosten einsparen, indem er die geforderte verkehrsübliche Sorgfalt kostengünstiger erreicht, denn hier haben die Opfer die restlichen Unfallkosten zu tragen. Im Gegensatz dazu muß bei der Gefährdungshaftung der Verursacher alle Schäden kompensieren. Deshalb hat er einen wesentlichen Anreiz, sowohl seinen Kenntnisstand über das Schadenpotential zu verbessern als auch die kostengünstigsten Sicherheitsstrategien zu ergreifen.[249] Es werden also unter der Gefährdungshaftung wesentlich stärkere Anreize bezüglich der Entwicklung und Implementierung von kostengünstigeren und effizienteren Sicherheitssystemen gesetzt, und damit ist sie auch unter dynamischen Effizienzgesichtspunkten der Verschuldenshaftung vorzuziehen.

Die Vorteilhaftigkeit der Gefährdungshaftung ist unter gewissen Umständen jedoch ambivalent. Unterstellt man bezüglich der Verschuldenshaftung der rechtsprechen-

---

245 Bei der Analyse bzgl. der effizienten Internalisierung externer Effekte werden rational handelnde und voll informierte Individuen unterstellt.

246 Für die Erfüllung des Effizienzkriteriums muß auch noch implizit unterstellt werden, daß das geforderte Sorgfaltsniveau entweder größer oder gerade gleich dem unter Gefährdungshaftung gewählten paretooptimalen Standard ist. Vgl. zum Beweis Koboldt, Leder und Schmidtchen (1992), S. 339.

247 Diesem Einwand kann bedingt begegnet werden, indem fallspezifisch nach der Learned-Hand-Formel Fahrlässigkeit bestimmt wird. Denn danach muß der Erwartungsschaden pL größer sein als die durch Sicherheitsvorkehrungen s entstandenen Aufwendungen C(s), jedoch sind die Informationsanforderungen einer solchen Entscheidungsregel für die rechtsprechende Instanz in vielen Fällen nicht zu erfüllen. Vgl. dazu u. a. Cooter (1991), S. 13ff.

248 Vgl. dazu auch Cansier (1993), S. 257f.

249 Hintergrund ist der Wettbewerbsdruck, durch welchen die verschiedenen Anbieter dazu angehalten werden, Innovationen in der Sicherheitstechnologie durchzuführen. Vgl. dazu Geißler (1993), S. 33.

den Instanz, daß sie in jedem Fall in der Lage ist, das gesamtgesellschaftlich optimale Ausmaß an Sicherheitsvorkehrungen s* auch in der Rechtsprechung durchzusetzen, und den Wirtschaftssubjekten, daß sie dieses geforderte Niveau auch realisieren, dann wird die Gefährdungshaftung bezüglich der Allokationseffizienz schlechter abschneiden, wenn die Verursacher die Schäden unterschätzen und nur einen Teil davon kompensieren müssen, weil sie als Verursacher nicht identifiziert werden können oder es sich um immaterielle, nicht ersetzbare Verluste handelt. Treten also mehrere Ursachen von Allokationsineffizienzen gleichzeitig auf, dann muß fallspezifisch entschieden werden, welches Haftungsregime effizienter ist.[250]

Wie gezeigt wurde, ist das Haftungsrecht dazu geeignet, die verschiedenen Allokationsineffizienzen hinsichtlich Sicherheits- und Vorsichtsmaßnahmen teilweise zu beheben, wobei die Gefährdungshaftung unter Vernachlässigung von Moral Hazard der Konsumenten bzw. Opfer stärkere Präventionsanreize bei den Verursachern bzw. Produzenten setzt. Die Schwächen des Haftungsrechts treten besonders dann zutage, wenn die Schuldzuweisung sich schwierig oder gar unmöglich gestaltet und die Verluste nicht zurechenbar, monetär schwer zu quantifizieren und vom Verursacher nicht zu kompensieren sind.[251]

Bei rational handelnden, vollständig informierten Wirtschaftssubjekten und in Abwesenheit von externen Effekten ist weder die Ressourcenallokation noch die Einkommensverteilung von den Haftungssystemen abhängig.[252] Jedoch hat sich schon bei der Bewertung der Allokationseffizienz der Produzentenhaftung angedeutet, daß Gefährdungs- und Verschuldenshaftung zu unterschiedlichen Ergebnissen hinsichtlich der Verteilung der entstandenen Schäden führt. Unter der Gefährdungshaftung werden über den einheitlichen Produktpreis, welcher die Aufwendungen für Sicherheitssysteme und Haftpflichtversicherungsprämien enthält, die Kosten auf alle Konsumenten gleichmäßig verteilt[253], wobei es aber dadurch zu einer Umverteilung innerhalb der Konsumentengruppe von denjenigen mit unterdurchschnittlichem auf diejenigen mit überdurchschnittlichem Schadenpotential kommt. Dagegen

---

250 Unterstellt man, daß auch das Opfer durch eigene Präventionsmaßnahmen den Erwartungsschaden reduzieren kann, ist die Verschuldenshaftung allokationseffizienter, weil sie sorgloses Verhalten von seiten der Geschädigten verhindert. Der Trend geht jedoch hin zur Gefährdungshaftung, weil Verschuldenshaftung und Fahrlässigkeit in einer automatisierten Welt ungeeignet sind. Vgl. dazu Viscusi (1984a), S. 10.

251 Vgl. zu einer allgemeinen Beurteilung des Haftungsrechts Cansier (1993), S. 268ff. Die angeführten Kritikpunkte werden bei der Eignungsuntersuchung des Haftungsrechts bzgl. der Risiken der Informationssicherheit in Kommunikationssystemen in Kapitel 2.7.3. explizit diskutiert.

252 Vgl. dazu Hamada (1976), S. 229.

253 Vgl. dazu Viscusi (1984a), S. 10f.

hat unter der Verschuldenshaftung bei Einhaltung des geforderten Sorgfaltsniveaus durch den Produzenten jeder Konsument den ihm entstehenden Schaden zu tragen. Somit kann daraus geschlossen werden, daß - zumindest in einer Gruppe von Konsumenten mit ähnlichen Schadenpotentialen - die Gefährdungshaftung eine gleichmäßigere und gerechtere Verteilung der Verluste durch Produktschadensfälle nach sich zieht.[254]

Im Rahmen des Deliktrechtes führt die Gefährdungshaftung zu einer umfassenden Internalisierung von durch Schadensfälle ausgelösten Externalitäten und damit zur Realisierung des Verursacherprinzips. Im Gegensatz dazu müssen unter der Verschuldenshaftung i. d. R. die Opfer den Schaden tragen, so daß es zu einer unerwünschten Durchbrechung des Verursacherprinzips kommt.[255]

Da die Durchsetzung und Abwicklung des Produkthaftungs- und des Deliktrechtes Transaktionskosten verursachen, muß neben einem Vergleich der allokativen und der distributiven Aspekte auch diese Komponente berücksichtigt werden. Die gesamten Verwaltungskosten des Haftungsrechtes belaufen sich auf die Summe aus der Anzahl der abgefundenen Ansprüche multipliziert mit den Durchschnittskosten und aus der Anzahl der eingeklagten Ansprüche mal den entsprechenden Kosten pro Rechtsstreit.[256] Die Verwaltungskosten - verursacht durch die Bereitstellung einer Haftpflichtversicherung - fallen relativ gering aus und werden deshalb wie die Kosten der Festsetzung und Kontrolle von Sorgfaltsniveaus und alle anderen Kostenarten in diesem Kontext vernachlässigt.

Im Vergleich der beiden Haftungssysteme läßt sich sowohl für die Produzentenhaftung als auch für die Haftung im Sinne des Rechts unerlaubter Handlungen generell folgendes feststellen:

1. Die Gesamtzahl der Rechtsansprüche wird unter der Gefährdungshaftung höher sein als unter Verschuldenshaftung. Denn bei der Gefährdungshaftung wird immer dann auf eine Kompensation bestanden, wenn der Schaden größer ist als die privaten Kosten, um einen Rechtsanspruch zu erheben, während bei der Verschuldenshaftung zusätzlich noch der Tatbestand der Fahrlässigkeit vorliegen muß.

---

254 Unterstellt man den Konsumenten einen abnehmenden Grenznutzen des Einkommens, dann steigert die gleichmäßige Verteilung der Unfallkosten durch die der Gefährdungshaftung immanenten Vollversicherung den Erwartungsnutzen der Nachfrager.

255 Hier muß noch einmal darauf hingewiesen werden, daß diese Argumentation nur gerechtfertigt ist, wenn die Opfer keine Mitverschuldungsmöglichkeit haben.

256 Vgl. dazu Shavell (1987), S. 262-276, und Cooter (1991), S. 24f.

2. Die Verwaltungskosten pro Schadensfall werden bei Verschuldenshaftung höher sein, weil zusätzlich zur Entschädigungssumme herausgefunden werden muß, ob es sich um fahrlässiges oder vorsätzliches Verhalten gehandelt hat, was erhebliche Kosten verursachen kann.

Aufgrund dieser beiden Tatbestände kann nicht eindeutig bestimmt werden, welches Haftungssystem letztendlich die geringeren Verwaltungskosten verursacht. Für die Verschuldenshaftung spricht die geringere Anzahl der zu entscheidenden Fälle, welche aber relativ höhere Kosten verursachen. Die Gefährdungshaftung ist zwar günstiger pro Schadensfall, da nicht der Tatbestand der Fahrlässigkeit oder des Vorsatzes geklärt werden muß. Es ist aber über eine größere Zahl von Rechtsansprüchen zu entscheiden, die jedoch allmählich bei einem verbesserten Sicherheitsniveau zurückgehen wird. Deshalb ist im Einzelfall zu beurteilen, welches Haftungssystem für den Staat kostengünstiger ausfällt.[257]

1.5.4 Besteuerung und Subventionierung

1.5.4.1 Begründungen und Ziele

Im vorangegangen Abschnitt wurde aufgezeigt, wie die Ausgestaltung des Haftungsrechts dazu beitragen kann, daß die Nebenbedingungen der Erwartungsnutzenmaximierung der Wirtschaftssubjekte so korrigiert werden, damit Anreize hinsichtlich eines wohlfahrtssteigernden Einsatzes von Sicherheitsgütern und -maßnahmen erzeugt werden können. Der eigentliche Grundgedanke der Pigou-Lösung ist, den Verursacher externer Kosten (Nutzen) unmittelbar so zu besteuern (subventionieren), daß die sozialen und privaten Grenzkosten bei der gesamtwirtschaftlich optimalen Marktgleichgewichtsmenge übereinstimmen. Dies kann durch die Besteuerung[258] (Subventionierung) bestimmter Güter erreicht werden, indem deren Nutzung bzw. die damit verbundenen Aktivitäten künstlich verteuert (verbilligt) werden. Der Preismechanismus des Marktes wird also lediglich korrigiert, aber nicht außer Kraft gesetzt. Vor allem bei der Internalisierung von negati-

---

[257] Trotz des Trends hin zur Gefährdungshaftung und eines gleichzeitigen Anstiegs der vor Gericht verhandelten Produkthaftungsfälle kommt Viscusi (1991), S. 74f, für die Situation in den Vereinigten Staaten zum Schluß, daß zwischen diesen beiden Phänomenen kein Zusammenhang besteht.

[258] Es wird hier vor dem Hintergrund der Steuer- und nicht der spezielleren Abgabenlösung argumentiert, so daß die Verwendungsseite der Steuereinnahmen vernachlässigt werden kann.

ven externen Effekten der Umweltnutzung hat dieses Instrument schon sehr früh in der ökonomischen Theorie solch eine Bedeutung erlangt, daß es sich im Laufe der ökologischen Umgestaltung der westlichen Industrieländer auch zu einem der wichtigsten umweltpolitischen Instrumente entwickelt hat.[259]

Bezüglich der Allokationsineffizienzen auf den Märkten für Sicherheitsgüter und -maßnahmen läßt sich der Einsatz von den Marktpreis korrigierenden Instrumenten wie folgt begründen. Die Hauptintention von Pigou-Steuern und Subventionen ist die Internalisierung externer Effekte, welche durch Sicherheitsvorkehrungen ausgelöst werden, und damit eine volkswirtschaftliche effiziente Allokation von Sicherheitsvorkehrungen.[260] Diese ist prinzipiell auf zwei Wegen erreichbar. Zum einen können Produkte, welche externe Schäden verursachen, gemäß ihrem externen Schadenpotential[261] besteuert werden, so daß durch einen Nachfragerückgang das auf andere Wirtschaftssubjekte übergreifende Schadenpotential reduziert wird. Zum anderen wird durch Subventionen der Erwerb von positive Externalitäten erzeugenden Sicherheitsgütern und -maßnahmen kostengünstiger, und dadurch kann ein höheres, wohlfahrtssteigerndes Präventionsniveau erreicht werden.[262]

Jedoch können diese Instrumente grundsätzlich auch die Fehlallokationen, welche von einzelnen Wirtschaftssubjekten aufgrund von asymmetrischer Informationsverteilung verursacht werden, beheben.[263] Unterstellt man den Wirtschaftssubjekten, daß sie das Gefahrenpotential aufgrund unzureichender Informationen unterschätzen, dann kann hier eine individuelle Wohlfahrtsverbesserung erreicht werden, indem riskante Aktivitäten durch spezielle Steuern verteuert und Sicherheitsmaßnahmen durch Subventionen verbilligt werden.[264]

---

259 Beispiele sind u.a. die Mineralölsteuer oder diverse Abwasserabgaben.

260 Mit besonderem Bezug auf die Externalitäten, die dadurch im Versicherungsbereich ausgelöst werden, haben Arnott & Stiglitz (1986) diese Lösungsmöglichkeit theoretisch untersucht.

261 Unter externem Schadenpotential wird die Differenz zwischen dem gesellschaftlich relevanten Erwartungsschaden ES_{sozial} und dem privaten Schadenpotential ES_{privat} verstanden.

262 Als Bemessungsgrundlage für die Subvention muß theoretisch die Differenz zwischen herangezogen werden. Dies ist der Unterschied zwischen der Verminderungen des sozialen und des privaten Erwartungsschadens durch die Ergreifung von Sicherheitsmaßnahmen ($\Delta ES_{sozial}(s)$ und $\Delta ES_{privat}(s)$). In der Praxis ist ein solches Verfahren nicht durchführbar.

263 Irrationales Verhalten unter Unsicherheit drückt sich durch eine falsche Verarbeitung der objektiv gegebenen Informationen aus, führt damit zu einer „falschen" Grenznutzenfunktion s* und kann deshalb durch die Besteuerung risikobehafteter Produkte und Aktivitäten nicht korrigiert werden, während auf die asymmetrische Informationsverteilung durch eine Beeinflussung der Determinanten der Grenznutzenfunktion s* direkt eingewirkt werden kann.

264 Als allgemeines Beispiel für die Besteuerung schädlicher Aktivitäten können die Tabak- und die Alkoholsteuer angeführt werden. Hingegen werden Tätigkeiten wie z. B. Weiterbildungsmaßnah-

Es ist also festzuhalten, daß sowohl die Besteuerung riskanter Aktivitäten als auch die Subventionierung von Sicherheitssystemen grundsätzlich die durch Externalitäten und asymmetrische Informationsverteilung verursachten Allokationsineffizienzen abzubauen vermögen.

1.5.4.2 Ausgestaltungsmöglichkeiten

Es wird zunächst darauf eingegangen, wie die Instrumente der Steuer- und der Subventionslösungen bezüglich der Behebung von Allokationsineffizienzen auf Märkten für Sicherheitsmaßnahmen speziell angewandt werden können.

Prinzipiell sind, wie bereits angeführt, zwei Vorgehensweisen zu unterscheiden. Die indirekte Strategie zur Internalisierung der Externalitäten von Sicherheitsvorkehrungen besteht darin, mittels der speziellen Besteuerung von riskanten Produkten bzw. Aktivitäten gemäß ihres für die Gesellschaft relevanten Schadenpotentials gleichzeitig mit ihrer umgesetzten Menge auch das dadurch generierte Schadenpotential zu reduzieren. Auf diesem Umweg wird die Diskrepanz zwischen der sozialen und der privaten Grenznutzenkurve von Sicherheitsmaßnahmen reduziert und damit c. p. die Fehlallokation als Differenz zwischen dem privaten und dem sozialen Optimum verringert. In Abbildung 6 wird dies als Linksverschiebungen der sozialen und privaten Grenznutzenkurven dargestellt. Dabei verschiebt sich die soziale Grenznutzenkurve stärker als die private nach links, weil auch der gesellschaftliche Schaden durch die Besteuerung stärker als der individuelle gesenkt wird.[265] Ferner läßt sich dies dadurch begründen, daß durch die steuerliche Belastung gerade die Ausbringungsmengen derjenigen Produkte am stärksten gesenkt werden, bei denen die Differenz zwischen sozialem und privaten Erwartungsschaden am größten ist, so daß in einer aggregierten Betrachtung die Differenz zwischen sozialem und privatem Schadenpotential zurückgeht. Die Besteuerung reduziert also die Divergenz zwischen sozialer und privater Grenznutzenfunktionen und damit auch das Ausmaß der Fehlallokation, welche in Abbildung 6 als Differenz von sozialem Optimum $s^{*\prime}_{sozial}$ und privatem Optimum $s^{*\prime}_{privat}$ definiert ist. Die Allokationsverbesserung wird auch durch die Verkleinerung des ursprünglichen gesellschaftlichen Wohlfahrtsverlustes in Form des hell schraffierten Dreiecks auf

---

men, deren zukünftiger Nutzen unterschätzt wird, steuerlich begünstigt und dadurch quasi subventioniert. Greenwald & Stiglitz (1986) haben die Eignung der Besteuerungs- und Subventionslösung sowohl bzgl. der Externalitätenproblematik als auch hinsichtlich Informationsasymmetrien und unvollständiger Märkte untersucht.

265 Es gilt nämlich $-\Delta ES_{sozial} > -\Delta ES_{privat}$.

das dunkel schraffierte Dreieck, welches den verbleibenden Wohlfahrtsverlust nach der Besteuerungslösung repräsentiert, deutlich.

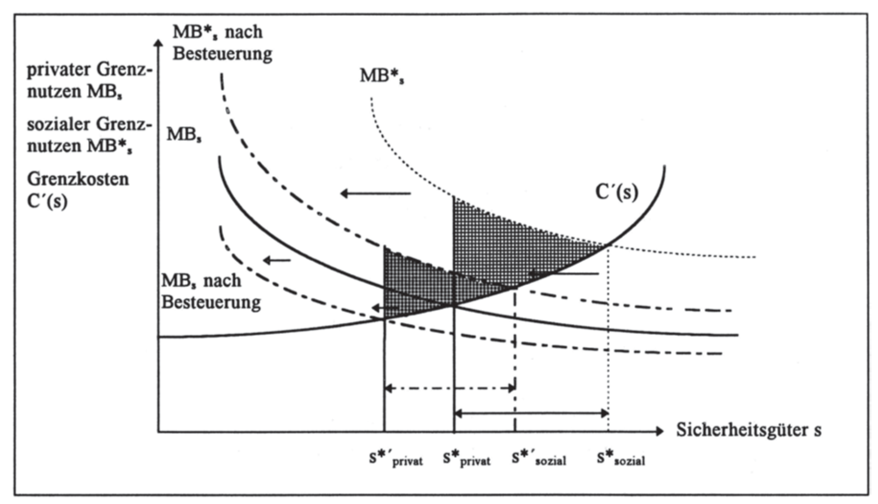


Abb. 6: Internalisierung negativer Externalitäten durch Besteuerung

Die gleiche Wirkungskette gilt bezüglich der Behebung von durch asymmetrische Informationsverteilung verursachten Fehlallokationen.[266] Allerdings wird hier nicht die Differenz zwischen sozialem und privatem Grenznutzen verringert. Die Besteuerung[267] und die daraus folgende Verminderung riskanter Aktivitäten werden den tatsächlichen Erwartungsschaden stärker reduzieren als den antizipierten.[268] Dadurch wird auch hier die Unterschiedlichkeit von tatsächlicher und antizipierter Grenznutzenfunktion abnehmen und damit das Ausmaß der durch diese Ursachen bedingten Fehlallokation zurückgehen. In Abbildung 7 wird dies wiederum dadurch verdeutlicht, daß nach der Besteuerung die Differenz, dargestellt als gestrichelter Doppelpfeil, zwischen dem realisierten s'_{privat} und dem optimalen privaten Sicherheitsniveau $s^{*\prime}_{privat}$ kleiner ausfällt als der Unterschied, abgebildet als durchgezogener Doppelpfeil, vor der Besteuerung (s_{privat} und s^{*}_{privat}) bzw. daß sich der gesellschaftliche Wohlfahrtsverlust in Höhe des hell schraffierten Dreiecks auf das dunkel schraffierte Dreieck reduziert.

---

[266] Es wird davon ausgegangen, daß der antizipierte Grenznutzen der Sicherheitsmaßnahmen aufgrund von Fehleinschätzung und -information geringer ist als ihr „wahrer" Grenznutzen.

[267] Als Steuerbemessungsgrundlage muß theoretisch die Differenz zwischen wahrem und wahrgenommenem Schadenpotential herangezogen werden.

[268] Hier sei unterstellt, daß die Fehlwahrnehmung weder vom Niveau des Erwartungsschadens noch von der Tatsache der Besteuerung beeinflußt wird.

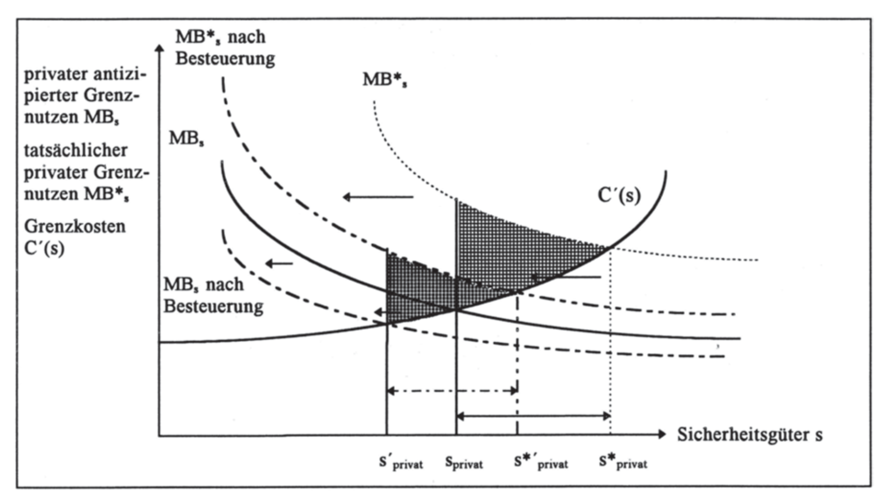


Abb. 7: Abbau von durch Informationsasymmetrien bedingten Allokationsineffizienzen durch Besteuerung

Anhand der Abbildungen 6 und 7 zeigt sich, daß die Besteuerung risikobehafteter Produkte gemäß ihrem externen bzw. nicht antizipierten Schadenpotential statisch betrachtet lediglich eine Verminderung der Fehlallokation auf dem Markt für Sicherheitsmaßnahmen herbeiführen kann, außer wenn ein prohibitiv hoher Steuersatz eingeführt wird, der die Nachfrage nach diesen Produkten vollständig zum Erliegen bringt. Dies ist jedoch durch den gleichzeitigen Verlust von Konsumenten- und Produzentenrenten nicht unbedingt wohlfahrtssteigernd. Deshalb sollte unter statischer Betrachtung die Höhe des Steuersatzes grundsätzlich so festgelegt werden, daß der zusätzliche Nutzengewinn aus dem Rückgang negativer Externalitäten und informationsbedingter Fehlallokationen den Verlust von Konsumenten- und Produzentenrenten gerade ausgleicht.

Die Besteuerungslösung ist lediglich eine Schadensverminderungsstrategie, welche die Gleichgewichtsmenge auf dem Markt für Sicherheitsgüter nicht unmittelbar beeinflussen kann. Sie vermag lediglich die von den Wirtschaftssubjekten für ihr individuelle Nutzenmaximierung antizipierten Nachfragedeterminanten den tatsächlichen und den für die Gesellschaft relevanten anzugleichen und dadurch nur indirekt das Ausmaß der Allokationsineffizienzen zu reduzieren.

Neben der indirekten Möglichkeit über die Besteuerung risikoreicher Aktivitäten kann eine unmittelbare Internalisierung positiver Externalitäten von Sicherheits-

vorkehrungen durch die Subventionierung der Anschaffungskosten C(s) erreicht werden.[269] In Abbildung 8 wird dies durch eine Verschiebung der Grenzkosten nach unten dargestellt. Dadurch, daß der Erwerb von Sicherheitssystemen verbilligt wird, steigt das ursprüngliche realisierte Präventionsniveau von s_{privat} auf s^*_{sozial} und entspricht damit dem Optimum an Sicherheitsvorkehrungen s*, in welchem die sozialen Grenzkosten und -nutzen ausgeglichen sind. Hier kann der optimale Subventionstarif direkt abgeleitet werden. Dargestellt als vertikaler Doppelpfeil sollte er so hoch ausfallen, daß durch die Subventionierung das gesellschaftliche Optimum an Sicherheitsmaßnahmen s* realisiert wird.

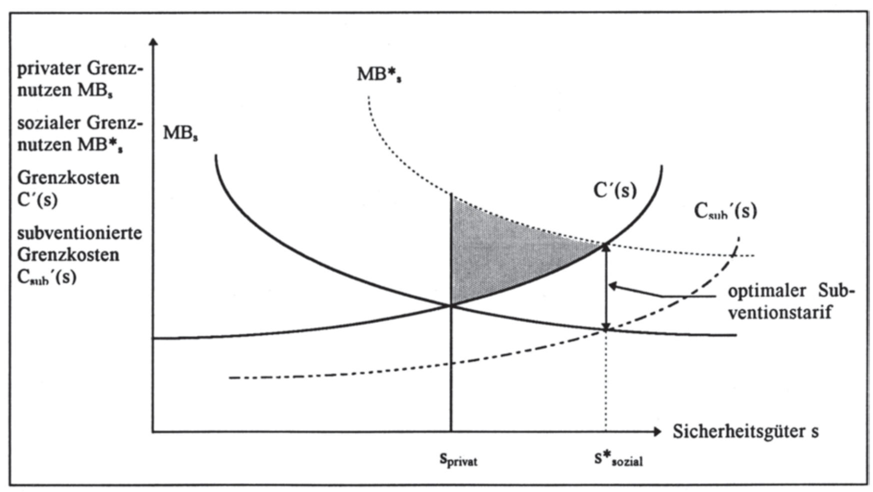


Abb. 8: Subventionierung von Sicherheitsgütern zur Internalisierung von Externalitäten

Durch eine Subventionierung von Sicherheitsmaßnahmen kann auch erreicht werden, daß das aufgrund asymmetrischer Informationsverteilung suboptimale Sicherheitsniveau s_{privat} sich dem optimalen Ausmaß s^*_{privat} anpaßt. Wie Abbildung 9 zeigt, senkt eine künstliche Verbilligung von Sicherheitsgütern die Grenzkosten,

[269] Arnott & Stiglitz (1986), S. 14, schlagen zur Reduzierung der Fehlallokationen, die im Zusammenhang mit Autounfällen stehen, u. a. vor, Kraftstoff und Alkohol zu besteuern und alternative Beförderungssysteme zu subventionieren.

und damit erhöht die daraus folgende Ausweitung der Sicherheitsmaßnahmen auch die individuelle Wohlfahrt der Wirtschaftssubjekte.[270]

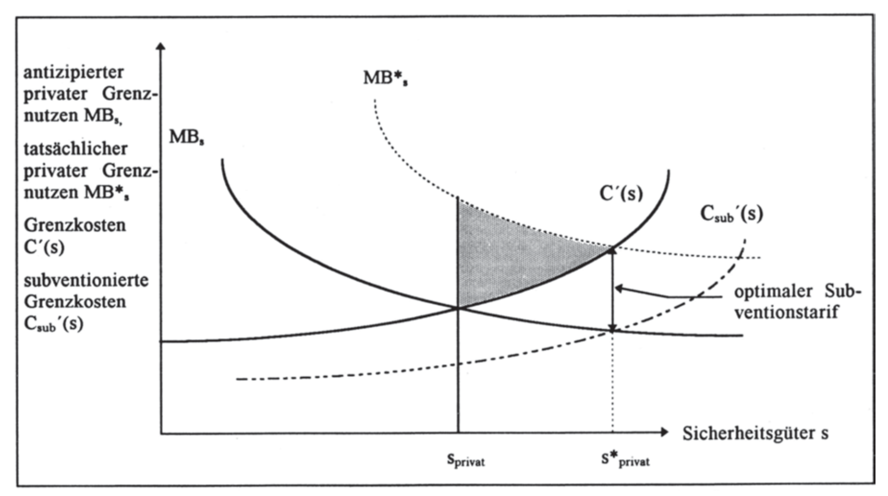


Abb. 9: Abbau von durch Informationsasymmetrien bedingten Allokationsineffizienzen durch Subventionierung

Das Subventionsverfahren sollte folgenden Anforderungen genügen.[271] Prinzipiell ist es anzustreben, die Subventionen direkt an die Betroffenen, d. h. in diesem Kontext an die Nachfrager nach Sicherheitsmaßnahmen, auszuzahlen. Jedoch kann es bedingt durch die Vielzahl der Nachfrager nach Sicherheitsmaßnahmen hinsichtlich des Verwaltungsaufwandes kostengünstiger sein, die Subventionen direkt an die Anbieter von Sicherheitssystemen und risikobehafteten Produkten auszuzahlen. Bei risikoreichen Anlagen und Aktivitäten spricht jedoch nichts gegen eine unmittelbare Auszahlung an deren Betreiber. Die Bemessungsgrundlage sollte so gewählt werden, daß sie mit dem zu fördernden Tatbestand, d. h. mit der Senkung des externen Schadenpotentials bzw. der Erzeugung positiver Externalitäten, kongruent ist.[272] Der Subventionsbetrag selbst errechnet sich dann aus dem Produkt

---

[270] Es sei darauf hingewiesen, daß sich die Informationsasymmetrie nicht auf die Marktpreise bezogen hat. Deshalb werden die Wirtschaftssubjekte die Subventionen korrekt antizipieren, so daß sich eine Allokationsverbesserung einstellen wird.

[271] Bei Subventionen i. e. S. handelt es sich eigentlich um Transferzahlungen an Unternehmungen. Hier umfaßt der Begriff Subvention auch Transfers an private Haushalte. Vgl. zum folgenden Andel (1992), S. 253ff.

[272] Vgl. dazu Fußnote 262. Dies ist zwar eine ökonomisch effiziente, aber keine realisierbare Subventionslösung, weil eine Quantifizierung der Bemessungsgrundlage nicht durchführbar ist. Vgl. zur Informationsproblematik den nächsten Abschnitt.

von Subventionsbemessungsgrundlage und Subventionstarif, dessen Höhe so festgesetzt werden sollte, daß sich das gesellschaftlich optimale Niveau an Sicherheitsmaßnahmen einstellt.[273] Schließlich kann man zwischen Empfangs- und Verwendungsauflagen unterscheiden, welche die Wirtschaftssubjekte berechtigen, eine Subvention zu erhalten. Aufgrund der schwierigen quantitativen Differenzierung von privatem und gesellschaftlichem Vorteil privater Sicherheitsgüter bietet es sich deshalb an, entweder den Erwerbern von Sicherheitssystemen einen bestimmten, im politischen Entscheidungsprozeß festgelegten Anteil des Kaufpreises zu kompensieren (Wertsubvention mit Empfangsauflagen) oder den Betreibern von risikoreichen Anlagen mittels Verwendungsauflage, welche die Installation von Sicherheitssystemen mit gewissem Mindestsicherheitsstandard fordert, eine finanzielle Unterstützung zu gewähren.[274]

1.5.4.3 Bewertung

Im Gegensatz zur Informationspolitik und dem Haftungsrecht wird bei der Bewertung der Pigou-Lösung hinsichtlich ihrer Allokationseffizienz das Gewicht vor allem auf der Problematisierung des dazu notwendigen Informationsaufwandes liegen.

Unterstellt man den staatlichen Instanzen, welche die Bemessungsgrundlagen und die Steuer- und Subventionstarife festzulegen haben, zunächst vereinfachend vollkommene Kenntnis der benötigten Grenznutzen- und Grenzkostenverläufe sowohl hinsichtlich risikoreicher Produkte und Aktivitäten als auch bezüglich der Sicherheitsmaßnahmen, dann kann die Pigou-Lösung zur Internalisierung von Externalitäten und der Behebung der informationsdefizitbedingten Fehlallokationen beitragen. Denn ein Steuer- bzw. Subventionssatz, der in der Höhe der Differenz zwischen sozialen und privaten bzw. wahren und antizipierten Grenznutzen festgesetzt ist, wird sowohl der statischen als auch der dynamischen Allokationseffizienz genügen.[275] Statisch betrachtet werden zum einen durch die Besteuerung risikoreicher

---

[273] Vgl. dazu die Abbildungen 8 und 9.

[274] Entsprechend §7 d Einkommensteuergesetz, der eine erhöhte Abschreibung für Wirtschaftsgüter, die dem Umweltschutz dienen, ermöglicht, bietet sich eine solche Subventionslösung auch für Sicherheitsgüter an.

[275] Vgl. dazu u. a. Fritsch, Wein und Ewers (1993), S. 73-85. Bezieht man, wie Greenwald & Stiglitz (1986), S. 237f, in die Untersuchung ein, daß die spezielle Besteuerung und Subventionierung von Gütern verzerrende Substitutionseffekte nach sich ziehen, dann müssen den Wohlfahrtsgewinnen durch Internalisierung die Wohlfahrtsverluste der verursachten Substitutionsprozesse („excess

Produkte Substitutionsprozesse hin zu sichereren Gütern und Anlagen ausgelöst und zum anderen durch die Subventionen Sicherheitssysteme verstärkt nachgefragt und implementiert. Dynamische Effizienz ist bei der Besteuerungslösung dadurch gegeben, daß die Anbieter der Produkte mit hohem externen bzw. mit nicht wahrgenommenem Schadenpotential durch den Nachfragerückgang dazu gezwungen werden, Aufwendungen für die Entwicklung von Sicherheitstechnologien zu unternehmen und ungefährlichere Produkte herzustellen, um am Markt bestehen zu können. Analog werden die Anbieter von Sicherheitssystemen, welche positive Externalitäten hervorrufen, durch die Subventionierung zu Lasten der übrigen Anbieter größere Marktanteile gewinnen, so daß auch die Subventionslösung dem Kriterium der dynamischen Effizienz genügen wird.[276] Durch die Besteuerung des Risikopotentials werden auch die Betreiber von risikoreichen Anlagen mit höheren Betriebskosten konfrontiert, die ihre Wettbewerbsfähigkeit schwächen und entweder eine Verdrängung aus dem Markt verursachen oder aus Kostengründen eine Installation von Sicherheitssystemen notwendig machen. Eine starke Subventionierung von Sicherheitssystemen kann dagegen Unternehmen zu Investitionen in risikoreiche Anlagen verleiten, weil u. U. überdurchschnittliche Gewinne erwartet werden. Jedoch werden auf die Installation von Sicherheitssystemen begrenzte Subventionen im allgemeinen nicht zu einer überdurchschnittlichen Investitionsrendite führen.[277]

Hebt man die strenge Annahme auf, daß den staatlichen Stellen die Verläufe der verschiedenen Grenznutzen- und Grenzkostenverläufe bekannt sind, dann ist die Treffsicherheit der Steuer- und Subventionslösung nur noch gering.[278] Dies bedeutet, daß es bei linearen Grenzkosten- und nicht-linearen Grenznutzenverläufen durch Preismodifikationen mittels Steuern und Subventionen zu beträchtlichen Fehlentwicklungen kommen kann.[279] Eng damit ist verbunden, daß mit diesen Instrumenten Allokationseffizienz nur dann erreicht werden kann, wenn die Differenz zwischen sozialer und privater Grenzkostenkurve im gesellschaftlichen Opti-

---

burden“ bzw. „deadweight loss“) entgegengestellt werden, so daß für gewöhnlich eine vollständige Internalisierung nicht zu einer effizienten Allokation aus gesamtwirtschaftlicher Sicht führen wird.

276 Die Subventionierung von Sicherheitsmaßnahmen kann jedoch auch negative Allokationsfolgen nach sich ziehen, wenn das höhere Sicherheitsniveau zusätzliche riskante Aktivitäten ermöglicht. Arnott & Stiglitz (1986), S. 10ff, schlagen unter bestimmten Umständen sogar eine Besteuerung vor.

277 Bei Altanlagen werden Subventionen für Sicherheitssysteme nicht erfolgreich sein, wenn zusätzlich zu den Anschaffungs- umfangreiche Umrüstungskosten anfallen. Vgl. zu dieser Problematik in Kommunikationssystemen Abschnitt 2.7.4.4.

278 Zur Kritik an der Pigou-Lösung bei Umweltproblemen, siehe u. a. Streissler (1993), S. 94ff.

279 Vgl. Weitzman (1974), S. 485ff.

mum bekannt ist. Ferner ist diese nur dann dieselbe wie im gegenwärtigen Zustand, wenn lineare Kurvenverläufe vorliegen. Die Informationsproblematik wird dadurch noch verschärft, daß es sich bei den Bemessungsgrundlagen im Gegensatz zu direkt festzustellenden Emissionswerten um nicht unmittelbar meßbare Erwartungsgrößen handelt und daß auch immaterielle Werte, wie Gesundheit und Leben, tangiert werden. Trägt man diesen Aspekten Rechnung, dann kann durch die Besteuerungs- und die Subventionslösungen in der Realität keine Allokationseffizienz, sondern lediglich eine Verringerung der Allokationsineffizienz erreicht werden. Aus Operationalitätsgründen können entweder risikoreiche Produkte mittels einer Wertsteuer um einen pauschalen Prozentsatz verteuert oder Sicherheitssysteme durch eine generelle Wertsubvention verbilligt werden. In beiden Fällen muß aus Vereinfachungsgründen der Nettoverkaufspreis als Bemessungsgrundlage dienen, weil externe bzw. nicht antizipierte Schadenpotentiale bzw. deren Veränderungen nicht zu quantifizieren sind.

Da die Besteuerung und die Subventionierung im Falle der Internalisierung positiver Externalitäten dem Verursacherprinzip gerecht werden, kann man von einer verteilungsgerechten Lösung sprechen. Eine Verminderung negativer Externalitäten durch die Subventionierung von Sicherheitssystemen in risikoreichen Anlagen durchbricht jedoch das Verursacherprinzip. Auch hinsichtlich der Informationsdefizite der Nachfrager entspricht nur noch die Besteuerung riskanter Produkte und Aktivitäten dem Verursacherprinzip. Dieses wird bei der Subventionslösung, welche die Folgen der Uninformiertheit der Konsumenten durch das finanzielle Engagement der Gesellschaft verhindern soll, nicht mehr realisiert. Zwischen informierten und uninformierten Konsumenten ist unter der Besteuerungslösung der Verteilungseffekt neutral, während die Subventionslösung den informierten Nachfragern Mitnahmeeffekte auf Kosten der dafür aufzukommenden Allgemeinheit einbringt, die ökonomisch nicht zu rechtfertigen und damit im politischen Entscheidungsprozeß auch nur bedingt durchzusetzen sind.

Schließlich ist der Verwaltungsaufwand der Besteuerungslösung beträchtlich, weil im Grunde für alle riskanten Produkte entsprechend ihrem externen bzw. nicht antizipierten Schadenpotential spezielle Steuern erlassen werden müssen, was sicherlich Akzeptanzprobleme bei den Steuerzahlern mit sich bringen wird.[280] Die Sub-

---

280 Unter Wohlfahrtsgesichtspunkten läßt sich deshalb ein staatlicher Eingriff mittels speziellen Steuern und Subventionen nur dann rechtfertigen, wenn die so gewonnenen Wohlfahrtsgewinne über den aufzuwendenden Verwaltungskosten liegen. Dieses zusätzliche Kriterium wird die Zahl staatlicher Interventionen merklich begrenzen.

ventionslösung hat im Vergleich dazu zumindest den Vorteil, daß nur die Produktgruppe der Sicherheitssysteme verbilligt werden muß, was eine wesentlich geringere Anzahl an Subventionsvergabeverfahren nach sich zieht.[281] Da die Anbieterseite sowohl die Subventionen erhalten[282] als auch die speziellen Steuern abzuführen haben, werden sich die Verwaltungskosten je Besteuerungs- bzw. Subventionstatbestand nicht wesentlich unterscheiden, so daß deshalb insgesamt die Subventionslösung für die Finanzverwaltung günstiger ausfällt und im Fall von positiven Externalitäten auch verteilungspolitisch zu rechtfertigen ist.[283] Generell handelt es sich bei diesen beiden Instrumente nicht um sich ausschließende Substitute, sondern um komplementäre Lösungsmöglichkeiten, welche jedoch die Verwaltungsstellen besonders bei einer Ausgestaltung, die sich den vollständigen Abbau der Fehlallokationen zum Ziel gesetzt hat, vor schwerwiegende Kontrollprobleme stellen.

1.5.5 Mindestsicherheitsstandards

1.5.5.1 Begründungen und Ziele

Das hinsichtlich von Produktsicherheitsrisiken am häufigsten angewandte Instrument staatlicher Regulierungspolitik ist das Erlassen von gesetzlichen Mindestsicherheitsstandards.[284] Hier handelt es sich um eine Möglichkeit der umfangreichen Klasse der Gebots- und Verbotslösungen, die entweder die Wirtschaftssubjekte unter Androhung von Sanktionen dazu zwingt, bestimmte Sicherheitsmaßnahmen zu ergreifen, oder die den Anbietern von Produkten mit Risikopotentialen nur dann eine Zulassung zum Markt gewährt, wenn gewisse Mindestanforderungen bezüglich der Produktsicherheit erfüllt werden.

---

[281] Zum selben Schluß kommt man, wenn unterstellt wird, daß die meisten Sicherheitsmaßnahmen dazu geeignet sind, gleichzeitig mehrere Arten von Schadensfällen zu verhindern.

[282] Die Auszahlung der Subventionen direkt an die Konsumenten und Nutzer bringt einen wesentlich höheren Verwaltungsaufwand mit sich, während die Einräumung der Abzugsfähigkeit von Ausgaben für Sicherheitsmaßnahmen von der Einkommensteuerbemessungsgrundlage ungewünschte regressive Verteilungseffekte verursacht.

[283] In dieser Analyse wird der fiskalische Aspekt, d. h. die Probleme der Verwendung der Steuereinnahmen und der Finanzierung der Subventionen, vernachlässigt. Vgl. allgemein zur Kritik an Subventionen Andel (1992), S. 255f.

[284] Vgl. zu Qualitätsstandards vor allem Viscusi (1984a), (1985), der besonders die Regulierungspraxis in den Vereinigten Staaten analysiert hat.

Mindestsicherheitsstandards sind grundsätzlich dazu geeignet, die negativen Folgen aller angeführten Ursachen von Allokationsineffizienzen hinsichtlich Sicherheitsmaßnahmen zumindest teilweise abzubauen. Irrationales Nachfragerverhalten als eine Form fehlender Konsumentensouveränität kann zwar nicht gänzlich verhindert werden. Jedoch können Fehlentscheidungen unter Unsicherheit, die eine suboptimale Nachfrage nach Sicherheitsmaßnahmen generieren, begrenzt werden, indem allen Wirtschaftssubjekten entweder unmittelbar oder mittels Produktsicherheitsnormen eine gewisse Zwangsnachfrage nach Sicherheitsvorkehrungen vorgeschrieben wird.[285] Dadurch werden sowohl ex ante das Produktrisiko, gemessen am Erwartungsschaden, als auch ex post der tatsächlich eingetretene Schaden vermindert[286], so daß sich die Differenz zwischen dem optimalen und dem realisierten Präventionsniveau verringert und damit der Umfang der durch Irrationalität bedingten Fehlallokation zurückgeht.

Fehlende Konsumentensouveränität kann sich auch in unzureichender und damit asymmetrischer Informationsverteilung zuungunsten der Nachfrager äußern.[287] Falls diese Informationsasymmetrien nicht durch andere Instrumente, wie durch Informationspolitik, soweit abgebaut werden können, daß keine bedeutenden Fehlallokationen mehr auftreten, dann bietet sich auch hier der Erlaß von Mindeststandards an.[288] Zwar vermögen sie nicht, die Informationsasymmetrie vollständig abzubauen, aber sie können den Nachfragern die Gewähr bieten, daß von den Anbietern ein Minimum an Sicherheitsvorkehrungen getroffen bzw. eine Begrenzung des Schadenpotentials vorgenommen wird.[289] Ein Mindestsicherheitsstandard schränkt also das mögliche Spektrum bezüglich der Vielfalt von Sicherheitsniveaus nach unten und bezüglich der Höhe des Schadenpotentials nach oben ein, so daß dadurch das Ausmaß möglicher Fehleinschätzungen indirekt begrenzt wird.

Schließlich hat sich die Setzung von Standards vor allem bei der Internalisierung externer Effekte in der Umweltpolitik bereits bewährt. Analog dazu sind auch Si-

---

285 In dieser Betrachtung wird vernachlässigt, warum Mindeststandards auch freiwillig zustande kommen können. Vgl. dazu z. B. Ault (1988).

286 Vgl. dazu Kuhlmann (1989), S. 180.

287 Nach Kuhlmann (1989), S. 177ff, steht hier nicht der wohl informierte Verbraucher, sondern der Durchschnittskonsument, der nur unzureichend über Schadenpotentiale und Schadenvermeidungsaktivitäten informiert ist, im Mittelpunkt der Analyse.

288 Vgl. dazu auch Fritsch, Wein und Ewers (1993), S. 200.

289 Als zusätzliches Kriterium bezüglich der Setzung von Mindestsicherheitsstandards führt Kuhlmann (1989), S. 179, die Tragbarkeit der Schäden an. Neben den externen Effekten ist für ihn vor allem die Irreversibilität von Schäden ein Argument für die Erlassung von Sicherheitsnormen.

cherheitsstandards grundsätzlich Instrumente, welche die in diesem Kontext existierenden Externalitäten zu internalisieren vermögen.[290] So können vor allem Fehlallokationen, welche durch externes Schadenpotential von riskanten Aktivitäten bzw. Gütern hervorgerufen werden, vermieden bzw. vermindert werden. Aber auch die positiven externen Effekte individueller Sicherheitsmaßnahmen können durch eine Zwangsnachfrage, z. B. in Form von obligatorischer Schutzimpfungen, realisiert werden.

Mindeststandards, die ein bestimmtes Sicherheitsniveau gewährleisten, sind also prinzipiell dazu geeignet, die nachfragebedingten Fehlallokationen auf den Märkten für Sicherheitsgüter und -maßnahmen zu begrenzen.

1.5.5.2 Ausgestaltungsmöglichkeiten

Um ein bestimmtes Minimum an Sicherheit zu erreichen, bieten sich grundsätzlich zwei Strategien an. Ist es technisch möglich, Sicherheitssysteme separat zu erwerben, dann können Wirtschaftssubjekte, die einer bestimmten Gruppe, wie die der Kraftfahrzeugbesitzer, angehören, dazu verpflichtet werden, bestimmte Sicherheitsvorkehrungen, z. B. ein Warndreieck, zu erwerben und in diesem Fall im Auto mitzuführen. Dies bedeutet, daß sie einem gewissen Nachfragezwang ausgesetzt sind, den sie nur unter der Gefahr einer Sanktionierung vermeiden können.[291] Jedoch haben sie für gewöhnlich eine gewisse Wahlmöglichkeit hinsichtlich Art und Ausstattung der Sicherheitsgüter. Wie in Kapitel 1.3 bereits aufgezeigt, sind jedoch in vielen risikoreichen Produkten bzw. Dienstleistungen Sicherheitsmechanismen bereits installiert, so daß dann ein unmittelbarer Zwang, bestimmte Sicherheitssysteme erwerben zu müssen, nicht realisierbar ist, sondern ein Produktsicherheitsstandard festgelegt wird, den der Anbieter bzw. Produzent erfüllen muß, um von einer staatlichen Instanz die Zulassungserlaubnis zum Markt zu erhalten. Da der zweite Fall sowohl in der Realität häufiger anzutreffen als auch Gegenstand der theoretischen Analysen ist, wird sich die detailliertere Darstellung der Ausgestaltungsmöglichkeiten und die sich daran anschließende Bewertung auf Produktsicherheitsstandards beziehen, wobei die allgemeinen Erkenntnisse auch auf die direkte Strategie, ein Mindestmaß an Sicherheitsvorkehrungen vorzuschreiben, übertragen werden können.

---

290 Vgl. dazu u. a. Dardis (1988), 307.

291 Faßt man auch die Versicherung die Sicherheitsstrategien, dann stellt die Versicherungspflicht ein vom Staat häufig verwendetes Instrument der Zwangsnachfrage dar.

Bezüglich obligatorischer technischer Standards läßt sich theoretisch folgende Unterscheidung treffen.[292] Die restriktiveren Objektnormen fordern von Produkten und Dienstleistungen bestimmte Sollwerte z. B. bezüglich Materialbeschaffenheit, während Ergebnisnormen lediglich verlangen, daß das Produkt unter bestimmten Bedingungen der Handhabung - d. h. gemeinhin in Testsituationen und Bedrohungsszenarien - gewisse Eigenschaften bzw. Ergebnisse vorzuweisen hat.[293] Damit bleibt dem Produzenten ein gewisser Handlungsspielraum, der ihm erlaubt, die für ihn kostengünstigste Konstruktion zur Erreichung des geforderten Resultats auszuwählen. In der Praxis ist diese strenge Trennung zwischen Ergebnis- und Objektnormen nicht immer möglich, da je nach Strenge der Definition des von der Anbieterseite akzeptierten Ergebnisstandards dieser letztendlich auch wie eine Objektnorm wirken kann.[294]

Weiterhin lassen sich Produktnormen danach unterscheiden, wie umfassend, d. h. wieviel Eigenschaften bzw. Funktionen bei einem Produkt erfüllt sein müssen, und wie anspruchsvoll sie sind. Hier lassen sich nach Kates (1976) vier Möglichkeiten unterscheiden, einen Sicherheitsstandard zu bestimmen. Erstens kann sich staatliche Regulierungspolitik grundsätzlich zum Ziel setzen, alle potentiellen Risiken zu vermeiden bzw. zu minimieren, ohne weitere Nutzen- und Kostenkomponenten in Betracht zu ziehen. Beispiele dafür sind die Verbote bestimmter Zusatzstoffe in Nahrungsmitteln. Etwas weniger restriktiv ist der Risikovergleich, der das Ziel hat, das Produkt bzw. die Produktvariante mit dem relativ geringsten Schadenpotential ausfindig zu machen und seine Sicherheitseigenschaften als generelles Minimalniveau festzusetzen. Eine nach ökonomischem Verständnis anspruchsvollere Methode ist die Risiko-Nutzen-Analyse, die den Nutzen eines Produktes oder einer Aktivität mit seinen verschiedenartigen Risiken zu vergleichen sucht. Höhere Schadenpotentiale sind für die Regulierungsbehörden dann akzeptabel, wenn ihnen entsprechend zusätzliche gesellschaftliche Vorteile gegenüberstehen. Die vierte Methode eines Kosten-Nutzen-Vergleiches, der die Wohlfahrtsgewinne einer Risikominderung ihren Kosten gegenüberstellt und der staatliches Handeln dann legitimiert, wenn letztere größer sind als die Kosten einer Reduktion des Schadenpoten-

---

292 Von Dienstleistungsanbietern wird für gewöhnlich eine Mindestqualifikationen, wie z. B. ein Meisterbrief gefordert, jedoch wird in diesem Kontext darauf nicht weiter eingegangen, weil es sich hier vor allem um technische Sicherheitsrisiken handelt.

293 Vgl. speziell dazu Kuhlmann (1989), S. 174f.

294 Vgl. dazu und dem folgenden Viscusi (1984a), S. 24ff.

tials, entspricht schließlich dem ökonomischen Prinzip der gesellschaftlichen Wohlfahrtsmaximierung.[295]

Schließlich können Sicherheitsstandards noch nach ihrem Anwendungsbereich differenziert werden. Die bedeutendsten Akzeptanzprobleme entstehen, wenn bereits genutzte Produkte nachträglich einem neu eingeführten Standard entsprechen sollen, weil kostenintensiven Rückrufaktionen und Konstruktionsveränderungen aufgrund der begrenzten Restlebensdauer eine oft nur geringe Nutzenkomponente gegenübersteht. Schwierig gestaltet sich auch die Modifikation bestehender Produktionslinien, weil wiederum immer noch beträchtliche Änderungskosten anfallen. Eher unbedenklich ist es dagegen, wenn Mindestsicherheitsstandards für noch zu entwerfende Produkte erlassen werden, so daß man daraus schließen kann, daß bei gleichem Nutzenzuwachs einer höheren Sicherheit pro Zeiteinheit die Ansprüche von Produktnormen mit zunehmendem Alter der Produkte abnehmen sollten.

Nach der Setzung von Standards müssen diese auch durchgesetzt werden.[296] Hier bieten sich generell zwei Durchsetzungsstrategien an. Entweder werden bei Entdeckung von Verstößen rigorose Geldstrafen verhängt, welche die Produzenten dann dazu veranlassen, die Standards einzuhalten, oder es werden nur gemäßigte Bußgelder festgesetzt, welche für manche Produzenten keinen Anreiz darstellen, sich um die Einhaltung der Produktnormen zu bemühen.[297] Letzteres ist ökonomisch gerechtfertigt, wenn die Umrüstungskosten für einen Produzenten höher sind als die Wohlfahrtsgewinne durch ein sichereres Produkt. Deshalb sollte sich die erwartete Strafe daran orientieren, welche Nutzengewinne sich für die Gesellschaft durch eine höhere Produktsicherheit ergeben. Auf diesem Weg ist durchaus die Einführung eines kosteneffizienten Standards möglich.

---

295 Eine Nutzen-Kosten-Analyse über die Sicherheitsgurtpflicht haben u. a. Arnould & Grabowski (1981) durchgeführt. Aufgrund monetär nicht quantifizierbarer Nutzenkomponenten ist man teilweise zum Kosten-Effektivitätsansatz übergegangen, der diejenige Schutzmaßnahme, die mit geringstem Aufwand ein bestimmtes Präventionsziel erreicht, als Mindestsicherheitsstandard festsetzt. Vgl. zu weiteren Problemen der Nutzen-Kosten-Analyse Crandall (1988), S. 65-73.

296 Haben sich die Wirtschaftssubjekte gegen die Risiken zusätzlich versichert, dann besteht für sie gewöhnlich ein unmittelbarer Anreiz, sich an die gesetzlich vorgegebenen Sicherheitsstandards zu halten, weil dies in vielen Versicherungsverträgen eine notwendige Bedingung darstellt, um im Schadensfall in den Genuß der vollständigen Versicherungsleistung zu kommen.

297 Die Durchsetzung kann auch danach unterschieden werden, ob ein strenges Zulassungsverfahren wie im Fall von Arzneimitteln existiert oder ob bei der Entdeckung von Verstößen Strafen verhängt werden. Vgl. dazu Kuhlmann (1989), S. 175f.

1.5.5.3 Bewertung

Hinsichtlich der Bewertung von Mindestsicherheitsstandards stehen vor allem ihre allokativen Wirkungen im Vordergrund, wobei zunächst allgemein die Effekte von Mindeststandards und danach genauer die von Produktsicherheitsstandards, differenziert nach den verschiedenen Implementierungsgründen, untersucht werden. Weiterhin wird neben der Darstellung der Verteilungseffekte der administrative Aufwand dieser Regulierungslösung einzuschätzen versucht.

Analog zu den Preissteuerungsinstrumenten kann die Allokationseffizienz von Standards in Abhängigkeit vom Kenntnisstand der Regulierungsbehörden bestimmt werden. Unterstellt man den standardsetzenden Instanzen, vollkommenes Wissen über den Verlauf der Grenzkosten- und Grenznutzenverläufe der verschiedenen Wirtschaftssubjekte, dann erfüllen Sicherheitsstandards auf einem Niveau, auf dem sich die sozialen bzw. antizipierten Grenznutzen und Grenzkosten jeweils ausgleichen, das Kriterium statischer Allokationseffizienz hinsichtlich aller drei nachfragebedingter Ursachen von Fehlallokationen nur dann, wenn innerhalb einer Gruppe potentieller Schadenverursacher identische Grenzkosten- und Grenznutzenfunktionen der Sicherheitsmaßnahmen unterstellt werden können.[298] Dynamische Effizienz wird durch sie im Gegensatz zu den Preisinstrumenten generell nicht erreicht, da die Wirtschaftssubjekte bei Ergebnisnormen zwar einen Anreiz haben, diese mit minimalem Aufwand zu erreichen, jedoch nicht sie zu übertreffen. Produktsicherheitsstandards werden also keine Innovationsanstrengungen hin zu verbesserten Sicherheitssystemen auslösen.[299] Materielle Objektnormen bieten den Individuen bzw. Produzenten nicht einmal die Möglichkeit, die für sie kostengünstigste Lösung auszuwählen.

Nimmt man das realistische Szenario an, daß bei den standardsetzenden Institutionen Unsicherheit über die tatsächlichen Grenzkosten- und Grenznutzenverläufe besteht, dann verursacht die Mengenregulierung bei flachem Verlauf der Grenzko-

---

[298] Statische Effizienz ist also selbst unter diesen unrealistischen Umständen ausgesprochen zweifelhaft, weil zusätzlich Homogenität der Wirtschaftssubjekte vorausgesetzt werden muß. Ein Mindeststandard ist deshalb nur dann eindeutig wohlfahrtssteigernd, wenn das optimale, alle Nutzenkomponenten integrierende Sicherheitsniveau s* aller Individuen darüber liegt.

[299] Grundsätzlich können staatliche Regulierungsaktivitäten die Innovationsanreize der Anbieter so verzerren, daß diese weniger Ressourcen in die Entwicklung neuer Produkte stecken und statt dessen sich verstärkt um die Einhaltung bzw. Mitgestaltung von Regulierungsvorgaben bemühen. Gray (1987) hat für die Vereinigten Staaten empirisch nachgewiesen, daß der Produktivitätsrückgang der US-Wirtschaft in den 70er Jahren zu einem Drittel der verstärkten Sicherheits- und Umweltregulierung zuzuschreiben ist. Vgl. allgemein zur Theorie der Regulierung u. a. Stigler (1971), Posner (1974) und Wilson (1980).

stenfunktion durchschnittlich zwar weniger Fehler als die preispolitischen Instrumente, aber der gewählte Sicherheitsstandard trifft meistens nicht das Niveau, das zur statischen Allokationseffizienz führt.[300]

Weitere Erkenntnisse lassen sich gewinnen, wenn man die Wirkungsweise von Mindestsicherheitsstandards bezüglich der verschiedenen Ursachen von Fehlallokationen differenziert. Extreme irrationale Verhaltensweisen bei der Schadensprävention können durch obligatorische Sicherheitsstandards mit Gewißheit verhindert werden, was vor allem bei gravierenden oder irreversiblen Schadenpotentialen angestrebt wird. Ähnlich ist ihre Wirkungsweise in Fällen asymmetrischer Informationsverteilung. Minimale Sicherheitsstandards führen dazu, daß der durch Informationsdefizite der Nachfrager mögliche Prozeß der adversen Selektion auf einem höheren Niveau zum Stillstand kommt.[301] Dies ist um so wohlfahrtssteigernder, je sicherheitsbewußter und unelastischer die Nachfrage ist, je geringer die Konsumenten den Mindestsicherheitsstandard bewerten und je geringer die Grenzkosten eines höheren Sicherheitsniveaus ausfallen.[302] Diesen positiven Aspekten muß entgegengehalten werden, daß das Angebotssegment mit weniger anspruchsvollen Sicherheitsausstattungen aus dem Markt gedrängt wird und gut informierte, rational handelnde und risikoliebende Wirtschaftssubjekte Wohlfahrtseinbußen hinnehmen müssen.[303] In der Regel dominiert aber die Gruppe der schlecht informierten risikoaversen Verbraucher, so daß deren Wohlfahrtsgewinne ausschlaggebend sind.[304] Schließlich ist hinsichtlich der Internalisierung von Externalitäten durch Sicherheitsstandards noch zu bemerken, daß wesentliche Wohlfahrtsgewinne nur dann zu erwarten sind, wenn jene keine Anreize zu risikoreicherem und unvorsichtigerem Verhalten auslösen.[305] Die Implementierung technischer Sicherheitssysteme kann - analog zu einer Vollversicherung - bestimmte Wirtschaftssubjekte zu sorglosem Verhalten verleiten, so daß das schließlich realisierte Sicherheitsniveau schlechter ausfällt als vor Einführung der Standards und damit bezüglich der dynamischen

---

300 Siehe Weitzman (1974), S. 485.

301 Vgl. dazu entsprechend die Ausführungen von Vahrenkamp (1991), S. 105, zu Qualitätsstandards.

302 Diese theoretischen Ergebnisse hat Leland (1979) bzgl. minimaler Qualitätsstandards abgeleitet.

303 Vgl. dazu Dardis (1977), S. 36ff, der die Wohlfahrtsverluste der statischen Analyse anhand verlorener Konsumentenrenten bestimmt. Längerfristig kann die Wettbewerbsintensität durch eine regulierungsbedingte Verminderung der Anbieter zurückgehen, was weitere Nachteile für die Nachfrager mit sich bringt.

304 Unterstellt man die Marktform der monopolistischen Konkurrenz, dann führt die Einschränkung der Produktvielfalt zur verstärkten Ausschöpfung der positiven Skalenerträge, was sich tendenziell in niedrigeren Produktpreisen niederschlagen wird. Vgl. dazu Viscusi (1984a), S. 22.

305 Vgl. dazu Risa (1992), S. 341, Crandall (1988), S. 72f, und Dardis (1988), S. 304f.

Effizienz keine Allokationsverbesserung sondern sogar eine -verschlechterung eintritt.[306]

Diese Verhaltensänderung einiger Wirtschaftssubjekte nach Einführung von Mindestsicherheitsstandards bringt neben ihren negativen Allokationsfolgen gleichzeitig unerwünschte Verteilungswirkungen mit sich. Denn die vorsichtig agierenden Wirtschaftssubjekte, die bedingt durch ihr Verhalten eigentlich keine zusätzlichen technischen Sicherheitssysteme bedürfen, werden durch Mindestsicherheitsstandards und der damit verbundenen Einschränkung des Angebot benachteiligt.[307] Nutznießer sind irrational handelnde und schlecht informierte Wirtschaftssubjekte, denen es durch die verbesserte obligatorische Sicherheitsausrüstung erst ermöglicht wird, noch höhere Risiken einzugehen.[308] Geht man weiterhin davon aus, daß sich nicht alle Wirtschaftssubjekte gleichermaßen durch irrationales Verhalten und Informationsdefizite auszeichnen, dann kommt es innerhalb der Gruppe der Nachfrager zu einer Umverteilung von den informierten, rational handelnden und risikoliebenden zugunsten der uninformierten, irrationalen und risikoaversen Wirtschaftssubjekte. All diejenigen, die sich ihrer intensiveren Sicherheitsbedürfnisse und ihrem Schadenpotential bewußt sind, werden von diesen Verteilungseffekten nicht betroffen. Schließlich müssen noch die Verteilungseffekte von Sicherheitsstandards, die durch die Internalisierung von externen Effekten erlassen werden, untersucht werden. Denn wird zur Internalisierung positiver externer Effekte von Sicherheitsmaßnahmen eine Zwangsnachfrage durchgesetzt, dann hat dies unerwünschte Verteilungskonsequenzen, weil der Verursacher die zusätzlichen Kosten zu tragen hat, obwohl der Nutzen anderen Gesellschaftsmitgliedern zufließt. Im Gegensatz dazu sind die Verteilungskonsequenzen von Produktsicherheitsstandards, die Externalitäten in Folge von Schadensfällen verringern und begrenzen, im Sinne des Verursacherprinzips.

---

306 Dieses dem Moral Hazard in der Versicherungsökonomie vergleichbaren Phänomen hat Peltzman, (1975), eindrücklich an der Einführung von Sicherheitsgurten in Automobilen nachweisen können. Weitere Beispiele mit ähnlichen Ergebnissen im Arzneimittelbereich hat Viscusi (1985) untersucht. Risa (1992) hat den Gesamteffekt einer Sicherheitsregulierung in einen direkten positiven Effekt und einen indirekten Effekt aufgespalten, der vor allem bei sehr risikoliebenden und extrem risikoaversen Individuen zu einer ungewünschten Reduktion des persönlichen Sorgfaltsniveaus führen kann.

307 Vgl. Crandall (1988), S. 72.

308 So verleitet das Antiblockiersystem der Bremsen von hochwertigen Kraftfahrzeugen manch einen Autofahrer zu schnellerem und damit gefährlicherem Fahren.

Der Verwaltungsaufwand für staatliche Institutionen, die Sicherheitsstandards bestimmen, erlassen, durchsetzen und schließlich auch kontrollieren, ist erheblich.[309] Zwar sind die Kosten der Regulierung mittels Standardsetzung im Einzelfall im Vergleich zum Haftungsrecht geringer, jedoch ist die Zahl der regulierenden Sachverhalte erheblich höher, weil bereits bei potentiellen Gefährdungen ein Regulierungsbedarf vorliegt. Außerdem muß vor Erlassen eines Standards je nach Strategie ein immenser Informationsbedarf befriedigt werden, der umfassende und gemeinhin kostenintensive Recherchen voraussetzt, vor allem wenn die regulierenden Instanzen bei ihrer Standardsetzung der dynamischen Entwicklung der Kosten- und Nutzenverläufe und den permanent neu entstehenden Gefahrenpotentialen gerecht werden wollen. Jedoch sind administrative Gebote und Verbote in Form von Mindeststandards grundsätzlich am einfachsten durchzusetzen und zu kontrollieren, weil Verstöße meist leicht festzustellen sind.[310] Im Umweltbereich hat sich aber gezeigt, daß Unsicherheit über die Auslegung und Durchsetzung von Standards leicht zu einer starken Erhöhung der Transaktionskosten zwischen regulierenden und regulierten Institutionen führen kann.[311]

1.5.6 Die staatliche Bereitstellung von Sicherheitsgütern und -leistungen

1.5.6.1 Begründungen und Ziele

Die extremste Form eines Eingriffs in den marktwirtschaftlichen Allokationsprozeß stellt die Bereitstellung öffentlicher Güter dar. In diesem Abschnitt wird zunächst begründet, unter welchen Bedingungen Sicherheitsgüter und -vorkehrungen durch den Staat angeboten werden sollten und unter welchen Umständen die private oder die staatliche Produktion günstiger ist. Schließlich erfolgt eine Bewertung dieses Instruments hinsichtlich der Allokationseffizienz und der Verteilungsgerechtigkeit.

---

309 Viscusi (1984a), S. 38, hat das Budget und die Beschäftigtenzahl der sicherheitsregulierenden Institutionen in den Vereinigten Staaten eruiert und kommt für 1982 auf über 25.000 Beschäftigte mit einem Gesamtbudget von über $6 Mrd..

310 Vgl. dazu Streissler (1993), S. 101. Verletzungen von Mindestsicherheitsstandards durch die Anbieter sind aber nicht immer zu beobachten. Deshalb werden inzwischen in Analysen der Regulierungstheorie auch die negativen Folgen von Informationsasymmetrien zwischen regulierter und regulierender Institution für das Allokationsergebnis berücksichtigt. Vgl. u. a. Chan & Marion (1994).

311 Vgl. dazu Cansier (1993), S. 213f.

Als Standardbeispiel eines reinen öffentlichen Gutes wird in den Lehrbüchern der Finanzwissenschaft oft die nationale Verteidigung angeführt, weil sowohl die Nichtrivalität im Konsum als auch die Nichtausschließbarkeit von Trittbrettfahrern, die aus einem rationalen Kalkül heraus nicht gewillt sind, ihre wahren Präferenzen für reine öffentliche Güter zu offenbaren, gegeben sind. Maßnahmen zum Schutz vor Bedrohungen durch äußere Feinde haben also den Charakter eines reinen öffentlichen Gutes und sollten deshalb aus Effizienzgesichtspunkten vom Staat zwar nicht unbedingt produziert, aber zumindest kostenlos bereitgestellt werden.

Dieser Spezialfall allein rechtfertigt jedoch nicht, daß die staatliche Bereitstellung von Sicherheitsgütern und -leistungen generell als Instrument zur Behebung der nachfragebedingten Allokationsineffizienzen dienen sollte.[312] So wird auch die Gewährleistung innerer Sicherheit, die dem Kriterium der Nichtausschließbarkeit streng genommen nicht genügt, schon seit Adam Smith als klassische Aufgabe des Staates betrachtet.[313] In diesem Fall wird der Einsatz der nicht marktkonformen und sehr ressourcenaufwendigen staatlichen Bereitstellung von marktfähigen Sicherheitsgütern vor allem durch die Externalitäten begründet, die annähernd den Charakter eines öffentlichen Gutes erreichen. Ferner entspricht das der Gesellschaft durch Kriminalität drohende Schadenpotential einem sogenannten öffentlichen Übel. Allgemein muß also bezüglich der Intensität der Externalitäten entweder gelten, daß die potentiellen Schäden weite Teile der Bevölkerung bedrohen, wodurch z. B. auch die staatliche Umweltschutzpolitik ihre Legitimation erfährt, oder die Wirkung eines Sicherheitssystems, wie der nationalen Streitkräfte, stiftet in einem solchem Maße positive externe Effekte, daß entweder grundsätzlich alle Gesellschaftsmitglieder[314] davon profitieren können oder der Nutzenanteil der in-

---

[312] Bei öffentlichen Gütern, die von allen Gesellschaftsmitgliedern in gleichem Maße genossen werden, kann man auch von einem Nachfragezwang sprechen. Da dies nur für den Spezialfall des globalen Klimas gilt und es den Wirtschaftssubjekten ansonsten möglich ist, zumindest den tatsächlichen Konsum von öffentlichen Gütern individuell zu gestalten, wird der staatlichen Bereitstellung von Sicherheitsvorkehrungen ein eigenständiger Abschnitt eingeräumt.

[313] Vgl. zu einer Effizienzanalyse der inneren Sicherheit Recktenwald (1967). Die ökonomischen Aspekte der Kriminalitätsbekämpfung werden jedoch in dieser Arbeit nicht weiter berücksichtigt. Vgl. zu einer Übersicht über die Kriminalitätsökonomie Kunz (1993).

[314] Falls nur eine begrenzte Zahl von Wirtschaftssubjekten betroffen ist, spricht man entweder bei Nichtausschließbarkeit von einem lokalen öffentlichen Gut oder bei Ausschließbarkeit von einem Clubgut.

dividuellen Sicherheitsvorkehrungen für das einzelne Wirtschaftssubjekt nur einen Bruchteil des gesellschaftlichen Nutzens ausmacht.[315]

Eine zweite Begründung für die staatliche Bereitstellung sind Informationsasymmetrien der Wirtschaftssubjekte hinsichtlich der Produktivität und Wirksamkeit von Sicherheitssystemen.[316] Eine Reihe staatlicher Dienstleistungen hat den Charakter von Vertrauensgütern, deren Qualität auch durch Erfahrung nicht überprüft werden kann. Deshalb bietet es sich an, diese Leistungen nach einem vorgegebenen und überprüfbaren Regelkatalog zu erstellen. Wird eine Leistung streng nach einem Regelsystem erstellt, dann haben private Anbieter meist keine Effizienzvorteile, sondern es ist u. U. gerade für eine staatliche Administration leichter, die Einhaltung der Vorgaben zu überprüfen.[317] Neben der Rechtsprechung fallen im Bereich der Sicherheitsvorkehrungen vor allem die nationalen Streitkräfte in diese Kategorie.[318] Zwar haben grundsätzlich alle Arten von Sicherheitsmaßnahmen den Charakter von Vertrauensgütern, weil sich ihre Qualität selbst nach einer längeren Erfahrungszeit nicht genau bestimmen läßt, wenn nicht genau zu ermitteln ist, ob ihre Wirksamkeit oder stochastische Einflüsse letztendlich für das Nichteintreten von Schadensfällen verantwortlich ist. Jedoch genügt nur die Erfüllung dieses Kriteriums für die Legitimation einer staatlichen Bereitstellung von Sicherheitssystemen nicht. Es muß sich bei diesen Systemen außerdem um Präventionsmaßnahmen handeln, die irreversible und durch Einzelpersonen bzw. -unternehmen nicht tragbare Risiken verhindern bzw. vermindern können.

Falls die staatliche Bereitstellung von Sicherheitssystemen den Charakter einer Zwangsnachfrage hat, dann könnten dadurch grundsätzlich auch irrationale Verhaltensweisen bei Entscheidungen unter Unsicherheit unterbunden werden. Da die

---

315 Vgl. dazu Oakland (1987), S. 496ff. Auf die Rolle von öffentlichen Gütern als Produktionsfaktoren wird hier nicht näher eingegangen, weil sich deren Problematik nicht wesentlich von der eines Konsumgutes unterscheidet. Vgl. dazu ebenda, S. 493f.

316 Faßt man ebenfalls Versicherungen unter Sicherheitsstrategien, dann kann die Bereitstellung einer staatlichen Versicherung auch dadurch gerechtfertigt werden, daß eine der Bedingungen für die Versicherbarkeit durch private Anbieter nicht erfüllt ist. Dieser Legitimationsversuch für eine staatliche Versicherung wird hier nicht weiter erläutert, sondern in Abschnitt 2.5.5 der Fallstudie als eine Lösungsmöglichkeit, um den Informationsrisiken von Kommunikationssystemen zu begegnen, näher untersucht.

317 Vgl. dazu Blankart & Pommerehne (1985), S. 439f.

318 Die Waffensysteme an sich können von privaten Unternehmen effizienter hergestellt werden, jedoch hat die Dienstleistung nationale Verteidigung Vertrauensgutcharakter und muß deshalb als öffentliches Gut bereitgestellt werden.

Zwangsnachfrage mittels Mindeststandards[319] im vorangegangenen Abschnitt bereits diskutiert wurde und die Wirtschaftssubjekte bezüglich öffentlicher Güter für gewöhnlich die Freiheit haben, diese auch nicht zu nutzen, wird die Bereitstellung öffentlicher Güter als ungeeignet für die Behebung irrationaler Verhaltensweisen angesehen und nicht weiter darauf eingegangen.[320]

1.5.6.2 Staatliche versus private Produktion von öffentlichen Sicherheitsgütern und -leistungen

Die Legitimierung der staatlichen Bereitstellung von Sicherheitsgütern und -leistungen durch Informationsasymmetrien oder positive Externalitäten bedeutet nicht zwangsläufig, daß der Staat auch für deren Produktion bzw. Erstellung verantwortlich sein muß.

Es bietet sich zwar unmittelbar an, daß der Staat die entsprechenden Sicherheitssysteme nicht nur als öffentliches Gut bereitstellt, sondern auch durch staatliche Unternehmen produzieren läßt.[321] Diese Vorgehensweise ist gerade dann vorteilhaft, wenn die Effizienz der Sicherheitsmaßnahmen nur begrenzt von Außenstehenden zu kontrollieren ist und die Folgen eines Defektes irreversibel und für die Gesamtwirtschaft von existentieller Bedeutung sind. Ist die Wirksamkeit von Sicherheitsmaßnahmen von staatlichen Kontrollinstanzen ohne bedeutenden Aufwand zuverlässig zu überprüfen, dann spricht zunächst das Ziel der Beschränkung der Staatstätigkeit in einer Marktwirtschaft für die private Produktion der Sicherheitssysteme.[322] Es kann also festgehalten werden, daß die Erstellung öffentlich bereitgestellter Sicherheitsmaßnahmen nur bei starken Informationsasymmetrien und existentiellen, volkswirtschaftlich relevanten Schadenpotentialen von staatlichen Institutionen durchgeführt werden sollte.

Unabhängig davon, wer letztendlich die öffentlich bereitgestellten Güter produziert, steht der Staat vor dem Problem, die optimalen Mengen von öffentlichen

---

319 Grundsätzlich erfüllen auch technische Standards die Kriterien von reinen öffentlichen Gütern, werden aber für gewöhnlich nicht von staatlichen Stellen erlassen. Vgl. dazu u. a. Kindleberger (1983).

320 Ausnahmen davon stellen die gesetzlichen Sozialversicherungen dar, für die ein Beitrittszwang besteht und deren Leistungen von den meisten Versicherten selbstverständlich in Anspruch genommen werden.

321 Die nationale Sicherheit wird in der Bundesrepublik Deutschland z. Zt. auch noch durch Dienstverpflichtung in Form der Wehrpflicht hergestellt. Vgl. dazu Blankart (1994), S. 75.

322 Auf die verschiedenen Verfahren der staatlichen Beschaffungspolitik wird nicht näher eingegangen. Vgl. dazu Andel (1992), S. 211ff.

Gütern zu bestimmen. Bei reinen öffentlichen Gütern ist es im Gegensatz zu privaten Gütern aufgrund der nicht durchführbaren oder nicht gewollten Nichtausschließbarkeit von zahlungsunwilligen Individuen nicht möglich, deren Präferenzen bzw. die aggregierte Zahlungsbereitschaft exakt zu ermitteln.[323] Deshalb kann auch das Allokationsoptimum an öffentlich bereitgestellten Sicherheitssystemen nicht exakt bestimmt werden.[324]

Neben der Mengenentscheidung ist ein Entschluß hinsichtlich der Preisfestsetzung zu fassen. Um die Gesamtwohlfahrt zu maximieren, muß der Preis der öffentlich bereitgestellten Sicherheitssysteme gleich den der Volkswirtschaft anfallenden Grenzkosten entsprechen. Handelt es sich um ein reines öffentliches Gut mit der Eigenschaft der Nichtrivalität im Konsum, dann sind die Grenzkosten zusätzlicher Nutzung gleich null und das Gut muß folgerichtig unentgeltlich angeboten werden, wobei die Erstellungskosten durch die allgemeinen Steuereinnahmen finanziert werden sollten. Treten dagegen ab einer bestimmten Nutzungsintensität Überfüllungskosten auf, dann müssen die Konsumenten mit einer entsprechenden Abgabe belastet werden.[325] Diese kann sinnvoller Weise nur dann erhoben werden, wenn kostengünstige Ausschlußtechniken existieren.[326]

1.5.6.3 Bewertung

Bei der Bewertung der staatlichen Bereitstellung von Sicherheitsmaßnahmen wird zunächst auf die allgemeinen Effizienzgesichtspunkte der Bereitstellung von öffentlichen Gütern eingegangen, bevor ein Vergleich zwischen der privaten und der staatlichen Produktion angestellt wird, der eine separate Untersuchung der Verwaltungskosten überflüssig macht. Schließlich konzentriert sich die Analyse der Ver-

---

323 Eine Zusammenstellung der verschiedenen Methoden der Präferenzerfassung für öffentliche Güter liefert Pommerehne (1987). Bezüglich der Nachfrage nach öffentlicher Sicherheit in den Vereinigten Staaten konnten Clark & Cosgrove (1990), mittels der Marktpreismethode zumindest die Einkommenselastizität ermitteln, während Clotfelter (1977), (1978) die Nachfrageelastizitäten bezüglich privater Sicherheitsmaßnahmen ermittelt. Anhand des Medianwähleransatzes hat Verhorn (1979), die Kreuzpreiselastizitäten zwischen privaten und öffentlichen Feuerschutzmaßnahmen bestimmt.

324 Für das Allokationsoptimum bei öffentlichen Gütern muß die Grenzrate der Transformation gleich der Summe der individuellen Grenzraten der Substitution sein. Diese Bedingung wird auch als „Samuelson-Rule" bezeichnet. Vgl. Samuelson (1954), (1955).

325 Vgl. dazu Oakland (1987), S. 500.

326 Der technische Fortschritt hat es bereits ermöglicht, daß eine Straßenbenutzungsgebühr je nach Verkehrsdichte erhoben werden kann.

teilungsaspekte auf das Verhältnis von Nutzungsintensität und finanzieller Belastung einzelner Wirtschaftssubjekte.

Grundsätzlich führt die Bereitstellung staatlicher Sicherheitsgüter und -leistungen, die aus dem allgemeinen Steueraufkommen finanziert werden, zu einer Steigerung der individuellen Erwartungsnutzen. Die Wohlfahrtssteigerung besteht darin, daß jeder durch seine Steuerzahlungen einen Anteil an den Gesamtkosten trägt, um in den Genuß des Schutzes vor bestimmten allgemeinen Risiken zu kommen. Unterstellt man den staatlichen Instanzen zunächst vollkommene Kenntnis über die Präferenzen der Individuen für die Sicherheitsgüter, dann wird soviel davon bereitgestellt, bis die Summe der Grenzraten der Substitution aller Gesellschaftsmitglieder gleich den jeweiligen Grenzkosten der Sicherheitsmaßnahmen ist.[327] Jedoch handelt es sich bei den individuellen Präferenzen um private Informationen, die für staatliche Institutionen unzugänglich sind, weil die Wirtschaftssubjekte meist keinen Anreiz haben, diese korrekt preiszugeben.[328] Zwar existieren eine Reihe von Verfahren zur Messung von Präferenzen für öffentliche Güter, jedoch hängt deren Genauigkeit vor allem auch davon ab, inwieweit die Individuen hinsichtlich der Sicherheitsgüter überhaupt fähig sind, rationale und informierte Entscheidungen zu treffen, was, wie in Kapitel 1.4 dargelegt, in vielen Fällen nicht gegeben sein dürfte.

Nachdem bereits die Ermittlung der optimalen Mengen von öffentlichen Gütern erhebliche Schwierigkeiten bereitet, stellt die Festsetzung effizienter Preise für die Nutzung dieser Güter ein zweites Problem dar. Bei Nichtanwendbarkeit des Ausschlußprinzips müssen die Erstellungskosten durch eine Steuerfinanzierung gedeckt werden, was jedoch nur dann allokationsoptimal ist, wenn die Grenzkosten der zusätzlichen Nutzung gleich null sind. Da dies aufgrund von Überfüllungserscheinungen für die meisten öffentlich bereitgestellten Güter nicht gilt, sind, um keine gesamtwirtschaftlichen Wohlfahrtsverluste zu erleiden, Benutzungsgebühren in Höhe dieser Grenzkosten zu erheben, was aber die Existenz von kostengünstig realisierbaren Ausschlußtechniken voraussetzt.

---

327 Dieses Effizienzkriterium gilt auch für Clubgüter und wird bezüglich Informationssicherheitsmechanismen in Kommunikationsnetzen in Abschnitt 2.5.4 der Fallstudie abgeleitet.

328 Falls sie befürchten, entsprechend ihrer Präferenzen zur Finanzierung herangezogen zu werden, dann ist es rational für sie zu untertreiben. Ein zusätzlicher, hier nicht weiter diskutierter Grund für eine nicht optimale Allokation von öffentlichen Gütern ist das Eigeninteresse der staatlichen Administration nach Budgetexpansion im Rahmen der Bürokratietheorie.

Somit ist deutlich geworden, daß sowohl die Bestimmung der Mengen als auch die Preisfestsetzung die staatlichen Instanzen vor große Schwierigkeiten stellen und es nur unter sehr restriktiven Bedingungen zur statischen Allokationseffizienz bezüglich öffentlicher Sicherheitsgüter kommen wird. Weiterhin kann die kostenlose bzw. -günstige Nutzung öffentlicher Sicherheitsvorkehrungen dazu führen, daß die Nachfrage nach substitutiven privaten Sicherheitsgütern vernachlässigt wird und dadurch auch das Kriterium der dynamischen Allokationseffizienz nicht erfüllt wird.

Besteht grundsätzlich die Wahlmöglichkeit, die Sicherheitsmaßnahmen privat oder staatlich herzustellen, wird ein Vergleich der Effizienz der Produktionstätigkeit im staatlichen und im privaten Sektor notwendig. Die private Produktion ist tendenziell kostengünstiger, weil die Gewinnmotivation und der Selektionsprozeß des Wettbewerbs die privaten Unternehmer dazu anhalten, die anfallenden Kosten zu minimieren, während die staatliche Bürokratie aus Prestigegründen eher dazu neigt, ihre Budget auszudehnen, und durch die Wähler und Politiker und fehlendem Konkursrisiko keine wirksame Kontrolle erfährt.

Bei der Erstellung vieler Vertrauensgütern bzw. -dienstleistungen ist jedoch von der privaten Produktion aufgrund der hohen Kosten der staatlichen Kontrollorganen bzw. der Unmöglichkeit der vertraglichen Fixierung von Leistungsinhalten abzusehen, so daß z. B. die nationale Verteidigung nicht von privaten Unternehmen geleistet werden kann. Neben diesen Schwierigkeiten sind die herrschenden Vergabeverfahren eine weitere Quelle der Ineffizienz bei der privaten Erstellung öffentlicher Leistungen.[329] Aufgrund des Ziels der Budgetmaximierung haben staatliche Einkäufer nicht unbedingt Anreize, den preisgünstigsten Angeboten den Zuschlag zu geben.[330] Weiterhin ist ihre Flexibilität durch Verwaltungsvorschriften geringer als die des privaten Beschaffungswesens. Durch die starke Lobby der in der jeweiligen Gebietskörperschaft ansässigen privaten Anbieter werden die staatlichen Stellen oftmals dazu gedrängt, die öffentlichen Aufträge an diese zu vergeben. Schließlich wird in Branchen, wie der Rüstungsindustrie, der Großteil des Umsatzes durch staatlichen Aufträge bestritten, so daß deren Lobby daraus eine staatliche Existenzsicherungsgarantie schließt, welche ohne Beachtung von Kostengesichtspunkten auch aus wahltaktischen Gründen gewährt wird.

---

329 Vgl. dazu u. a. Andel (1992), S. 210f, und Blankart (1994), S. 425ff.

330 Da die staatlichen Bürokraten nicht nach ihrer Fähigkeit zum Kosteneinsparen entlohnt werden und bei Fehlentscheidungen für gewöhnlich nicht von Kündigung bedroht werden, sind auch die individuellen Leistungsanreize im Vergleich zum privaten Sektor gering.

Unter Vernachlässigung der polit-ökonomischen Argumente lassen sich hinsichtlich der Verteilung folgende Aussagen treffen. Verteilungsgerechtigkeit ist dann gegeben, wenn die Wirtschaftssubjekte entsprechend ihrer Präferenzen bzw. Nutzungsintensität für die Finanzierung der öffentlich bereitgestellten Sicherheitsgüter aufkommen. Da bei reinen öffentlichen Gütern die konsumierte Menge für alle Individuen gleich ist, muß der Finanzierungsbeitrag gemäß den individuellen Präferenzen erhoben werden.[331] Dies ist aufgrund der Präferenzverschleierungsanreize in aller Regel nicht möglich, so daß durch die Ersatzlösung der allgemeinen Steuerfinanzierung sowohl die risikoaversen als auch die Gesellschaftsmitglieder mit hohen Schadenpotentialen bevorzugt werden. Deren Begünstigung fällt um so stärker aus, desto intensiver der private Charakter der staatlichen Sicherheitssysteme ist bzw. je geringer die positiven Externalitäten sind. In diesem Falle bietet es sich auch bei fehlenden Überfüllungskosten an, einen Teil der Finanzierung über Benutzungsgebühren zu bestreiten, weil somit die Äquivalenz von erhaltender Leistung und geleistetem Beitrag verbessert wird.[332]

Die Untersuchung der staatlichen Bereitstellung von Sicherheitssystemen hat ergeben, daß diese Lösung nur bei beachtlichen positiven Externalitäten oder bei Informationsdefiziten hinsichtlich der Effizienz der Sicherheitssysteme in Verbindung mit irreversiblen und durch Einzelpersonen nicht tragbaren Schadenpotentialen gerechtfertigt ist, weil die Mengen- und Preisfestsetzung durch staatliche Instanzen beträchtlichen Unzulänglichkeiten unterliegt, wobei aus Effizienzgesichtspunkten die private Produktion bevorzugt werden sollte, außer wenn erhebliche Schwierigkeiten bei der Kontrolle der von privaten Herstellern zu liefernden Sicherheitsleitungen auftreten.

1.5.7 Zusammenfassende Bewertung aller staatlichen Instrumente

Dieses Kapitel schließt mit einer zusammenfassenden Bewertung der fünf vorgestellten staatlichen Instrumente zur Behebung der nachfragebedingten Allokationseffizienzen auf den Märkten für Sicherheitsgüter und -maßnahmen. Zwar werden diese bereits in den einzelnen Abschnitten hinsichtlich Allokationseffizienz, Vertei-

---

331 Vgl. dazu Blümel, Pethig und von dem Hagen (1986), S. 260.

332 In den Vereinigten Staaten werden die lokalen Polizeikräfte aus dem Aufkommen der „property tax" finanziert. Damit werden Gemeindemitglieder mit größeren Häusern, die durch kriminelle Straftaten in einem höheren Ausmaß geschädigt werden können, stärker belastet, so daß dadurch das Äquivalenzprinzip realisiert wird. Vgl. Schwab & Zampelli (1987).

lungsgerechtigkeit und Verwaltungsaufwand beurteilt, aber um ein Gesamturteil fällen zu können, muß ein Bewertungsschema zugrunde gelegt werden. Zunächst werden die verschiedenen Instrumente in Übersicht 3 nach ihrer Allokationseffizienz bei der Beseitigung von irrationalem Verhalten, von Informationsasymmetrien und von Externalitäten bewertet, wobei in diesem qualitativen Bewertungsschema hoch (++) eine gute Eignung bedeutet, während mittel (+) andeutet, daß nur bedingt eine Verbesserung zu erwarten ist, und gering (0) vollständige Untauglichkeit signalisiert.

Instrumente	**Ausgestaltungsformen**	**Allokationseffizienz auf Sicherheitsmärkten**			**Gesamtbewertung der Allokationseffizienz**
		Irrationalität	Informationsasymmetrien	Externalitäten	
Staatliche Informationspolitik	Screening	gering(0)	hoch (++)	gering (0)	++
	Signaling	mittel (+)	mittel (+)	gering (0)	++
Haftungssysteme	Gefährdungshaftung	hoch (++)	hoch (++)	hoch (++)	++++++
	Verschuldenshaftung	mittel(+)	mittel (+)	mittel (+)	+++
Preisanreize	Besteuerung	gering(0)	mittel(+)	mittel (+)	++
	Subventionen	gering(0)	mittel(+)	mittel (+)	++
Staatliche Mengenregulierung	Mindestsicherheitsstandards	hoch (++)	mittel (+)	mittel (+)	++++
Staatliche Bereitstellung	staatliche Produktion	gering(0)	mittel(+)	hoch (++)	+++
	private Produktion	gering(0)	mittel(+)	hoch (++)	+++

Übersicht 3: Allokationseffizienz der staatlichen Instrumente

Die höchste Tauglichkeit hinsichtlich aller drei Marktversagensursachen erreicht die Gefährdungshaftung, gefolgt von den umfassend wirksamen Mindestsicherheitsstandards. Weniger und eigentlich nur bei Sicherheitsgütern und -leistungen mit starken positiven Externalitäten geeignet ist die staatliche Bereitstellung. Bedingt zweckmäßig zur Allokationsverbesserung sind schließlich die Mittel der staatlichen Informationspolitik und die Steuer- bzw. Subventionslösungen.

Zusätzlich zur Allokationseffizienz gehen, wie in Übersicht 4 auf der folgenden Seite dargestellt, in die Bewertung der einzelnen Instrumente auch die Verteilungsgerechtigkeit und der beim Staat entstehende Verwaltungsaufwand ein. Innerhalb des Gesamturteils hat die Allokationseffizienz ein Einfluß von 60%, während Verteilungsgerechtigkeit und Verwaltungsaufwand jeweils mit 20% in die Gewichtung einfließen.[333]

In der Endbewertung nimmt wiederum die Gefährdungshaftung die Spitzenposition ein, weil sie auch sowohl hinsichtlich Verteilungsgerechtigkeit und Verwaltungsaufwand gut abschneidet. Deshalb erweist sich letztendlich auch das Signaling der Informationspolitik ähnlich günstig, gefolgt von den verwaltungsaufwendigen Mindeststandards und der staatlichen Bereitstellung privat produzierter Sicherheitsgüter. Als in der Regel eher ungenügend müssen die Preisanreize und die staatliche Produktion und Bereitstellung von Sicherheitsmaßnahmen angesehen werden.

[333] Diese willkürliche Gewichtung bietet sich deshalb an, weil drei Ursachen von Allokationsineffizienz vorliegen und damit ohne Umrechnung die Ergebnisse aus Übersicht 3 übernommen werden können.

Instrumente	Ausgestal-tungsformen	Bewertungskriterien			Gesamt-bewertung
		Allokations-effizienz	Verteilungsge-rechtigkeit	Verwal-tungs-aufwand	
Informations-politik	Screening	mittel-gering (++)	mittel (+)	mittel (+)	++++
	Signaling	mittel-gering (++)	hoch (++)	klein (++)	++++++
Haftungs-systeme	Gefähr-dungshaftung	hoch (++++++)	hoch (++)	groß (0)	++++++++
	Verschul-denshaftung	mittel (+++)	mittel (+)	groß (0)	++++
Preis-anreize	Besteuerung	mittel-gering (++)	hoch (++)	groß (0)	++++
	Subven-tionen	mittel-gering (++)	mittel (+)	groß (0)	+++
Staatliche Mengenre-gulierung	Mindests-sicherheits-standards	mittel-hoch (++++)	mittel (+)	groß (0)	+++++
Staatliche Bereitstellung	staatliche Produktion	mittel (+++)	mittel (+)	groß (0)	++++
	private Pro-duktion	mittel (+++)	mittel (+)	mittel (+)	+++++

Übersicht 4: Gesamtbewertung der staatlichen Instrumente

In der Praxis werden gemeinhin mehrere Instrumente gleichzeitig eingesetzt, weil in vielen Situationen Allokationsineffizienzen durch mehrere der dargestellten Ursachen vorliegen. Ferner stehen die verschiedenen Instrumente nicht in einem substitutiven, sondern in einem komplementären Verhältnis. Gegenstand theoreti-

schen Interesses sind vor allem die Interdependenzen zwischen dem Haftungsrecht und staatlicher Regulierungsinitiativen in Form von Mindeststandards.[334] Eine umfassende Analyse aller möglichen Kombinationen von Marktversagensursachen und des entsprechenden Instrumentenmixes wird hier jedoch nicht vorgenommen. In der folgenden Fallstudie über die Informationssicherheit in Kommunikationssystemen wird nach der jeweiligen Darstellung und Bewertung der einzelnen Instrumente in Abschnitt 2.7.7 versucht, die Beziehungsverhältnisse zwischen den verschiedenen Instrumenten aufzuzeigen und daraus einen Policy-Mix abzuleiten.

334 Vgl. u. a. Shavell (1984), (1984a) und Kolstad, Ulen und Johnson (1990).

2. Teil: Informationssicherheit in Kommunikationssystemen: Allokationsineffizienzen und Lösungsmöglichkeiten

2.1 Vorbemerkungen zum Vorgehen

Nachdem im ersten Teil der Arbeit allgemein das Allokationsoptimum auf den Märkten für Sicherheitsgüter und -maßnahmen bestimmt worden ist, potentielle nachfragebedingte Gründe für Allokationsineffizienzen identifiziert und schließlich geeignete staatliche Instrumente zur Allokationsverbesserung untersucht wurden, wird im zweiten Teil der Arbeit eine spezielle Anwendung dieser Vorgehensweise und der gewonnenen Erkenntnisse auf die Problematik der Informationssicherheit in offenen, d. h. für die Allgemeinheit zugänglichen Kommunikationsnetzen durchgeführt.[335]

Die Auswahl des Themenbereiches der Fallstudie begründet sich durch folgende aktuelle Tatbestände.[336] Zunächst ist die Mehrheit der Bevölkerung durch Informationssicherheitsrisiken, d. h. beabsichtigte oder zufällige Beeinträchtigungen von Kommunikationsbeziehungen, in Kommunikationsnetzen bedroht, weil nahezu jedes Individuum an das Telefonfestnetz angeschlossen ist[337] und viele auch einen Zugang zu den diversen Mobilfunknetzen haben. Weiterhin werden sich in naher Zukunft vor allem durch die Aufbrechung der bisherigen staatlichen Monopole viele neuartige Kommunikationsnetze und -dienste etablieren[338], so daß der Umsatz des Telekommunikationsmarktes den des Automobilmarktes überholen und im Vergleich zu der sich schon nahe an der Sättigungsgrenze befindenden „klassischen" Computerindustrie weiter an relativer Bedeutung zunehmen wird. So wurden in der Bundesrepublik Deutschland seit 1990 pro Jahr 0,8% des Bruttoinlandproduktes in den Telekommunikationssektor investiert.[339] Auf dem Markt für

---

[335] Es werden also keine geschlossenen unternehmensinternen, sondern nur sogenannte offenen Netze betrachtet. Vgl. zur Ökonomie offener Netzwerke u. a. Weinkopf (1993).

[336] Sicherheitsökonomische Analysen richteten sich in der Vergangenheit vor allem auf die Bereiche Arbeitsschutz, Verbraucherschutz im Bereich von Nahrungs- und Arzneimitteln und Verkehrssicherheit. Vgl. dazu Viscusi (1992) und Jones-Lee (1989).

[337] Im Jahre 1992 gab es in der Bundesrepublik über 35 Millionen Telefonanschlüsse. Vgl. dazu Barth (1992), S. 48. Weltweit existieren z. Zt. nahezu 1 Mrd. Anschlüsse an Sprechnetze mit einer jährlichen Wachstumsrate von ca. 4%. Vgl. dazu von Schau (1994), S. 147.

[338] Vgl. das Eckpunkte-Papier über den zukünftigen Regulierungsrahmen im Telekommunikationsbereich der Bundesrepublik Deutschland vom Bundesministerium für Post und Telekommunikation (1995), welches keine zahlenmäßige Beschränkung der Lizenzen für Netz- und Dienstebetreiber vorsieht.

[339] Vgl. o. V. (1994b).

Kommunikationsdienste und elektronische Medien wurden 1993 90 Mrd. DM umgesetzt.[340] In den USA erzielte die Telekommunikationsindustrie nach einer Steigerung von 29% zum Vorjahr 1994 über 50 Mrd. US$ Umsatz.[341] Weitere Schlagzeilen über enorme Wachstumszahlen in dieser Branche sind permanent der Tagespresse zu entnehmen.

Gleichzeitig sind mit dieser Marktexpansion die Risiken und Bedrohungen, die durch die Nutzung der verschiedenen Kommunikationssysteme hervorgerufen werden, beträchtlich angestiegen, so daß Schätzungen von durch Computerkriminalität verursachten weltweiten Schäden in Höhe von fünf Milliarden Dollar pro Jahr ausgehen.[342] Konsequenterweise nehmen deshalb mittlerweile unter den Sicherheitsgütern Systeme zur Sicherung der Informationsvermittlung einen bedeutenden Platz ein.[343] In der Bundesrepublik Deutschland hat der Staat schon frühzeitig darauf reagiert und das Bundesamt für Sicherheit in der Informationstechnik (BSI) geschaffen, das zwar vor allem den Sicherheitsbedürfnissen des Bundes nachkommen soll, aber auch allgemeine Forschungsarbeit leisten und privaten Anbietern oder Nachfragern Unterstützung gewähren kann.[344]

Mit der Zunahme der realen Bedeutung der Kommunikations- und Informationstechnologie haben die damit verbundenen Gefahren und Risiken bereits das Interesse von Sozial- und Rechtswissenschaftlern[345] geweckt. Neben der großen realwirtschaftlichen Bedeutung ist die Thematik aber auch von besonderem theoretischem ökonomischem Interesse, weil es sich bei Kommunikationsnetzen und -diensten nicht um rein private Güter, sondern, wie noch zu zeigen ist, um sogenannte Clubgüter handelt, und weil die Bedrohungen der verschiedenen Aspekte der Kommunikationssicherheit nicht nur monetäre, sondern auch immaterielle Konsequenzen nach sich ziehen, so daß die theoretische ökonomische Analyse dieses Problembereichs eine besondere Herausforderung darstellt. Ferner sind der Problematik der Informationssicherheit in Kommunikationssystemen asymmetrische Informationsverteilungen und Externalitäten immanent, die Allokationsineffi-

---

340 Vgl. o. V. (1995).

341 Vgl. o. V. (1995a).

342 Vgl. Netzer (1995), S. 82.

343 Die Deutsche Telekom AG hat bereits 1988 mit TeleSec ein Projekt ins Leben gerufen, welches dem wachsenden Sicherheitsbedürfnis im Telekommunikationsbereich Rechnung tragen soll. Vgl. dazu Wolfenstetter (1991). Nach einer Studie von Frost & Sullivan beträgt der europäische Markt für Sicherheit in der Informationstechnologie 1995 über 2 Mrd. $. Allein für den Umsatz der Produkte der Netzwerk-Sicherheit werden 145 Millionen $ veranschlagt

344 Vgl. BGBl. S. 2834 vom 17. 12. 1990.

345 Vgl. u. a. Roßnagel, Wedde, Hammer und Pordesch (1989) und Wildhaber (1993).

zienzen in einem Ausmaß hervorrufen können, welche einen Einsatz der bereits dargestellten staatlichen Instrumente der Sicherheitspolitik rechtfertigen.

Nach einem aktuellen Überblick über die Kommunikationsnetze und -dienste in der Bundesrepublik Deutschland werden ausgehend von der Identifikation der allgemeinen ökonomischen Eigenschaften von Kommunikationsnetzen und -diensten die Eigenschaften eines optimalen Kommunikationsclubs bestimmt. Darauf aufbauend wird das volkswirtschaftlich effiziente Ausmaß an Informationssicherheit für das jeweilige Kommunikationssystem abgeleitet. Als Grundlage dafür werden zuvor die Gefahrenpotentiale für die Informationssicherheit kurz charakterisiert, die Probleme der Bewertung ihres Nutzens bzw. der Schadensfälle bei Verletzungen der Informationssicherheit diskutiert und die Kosten der Informationssicherheitsmechanismen in Abhängigkeit von den Netzeigenschaften bestimmt. Danach erfolgt eine kritische Darstellung einer anderen Präventionsmöglichkeit, nämlich der Versicherung gegen Informationssicherheitsrisiken in Kommunikationssystemen. Hier schließt sich die Untersuchung der Frage an, ob ein staatlicher Eingriff in dieses Segment des Versicherungsmarktes gerechtfertigt werden kann. Hinsichtlich der Implementierung von Informationssicherheitsmechanismen in offenen Kommunikationsystemen werden Ursachen von Allokationsineffizienzen identifiziert. Es folgt vor dem Hintergrund der institutionellen und rechtlichen Gegebenheiten in der Bundesrepublik Deutschland die Darstellung verschiedener staatlicher Instrumente zur Behebung der festgestellten Allokationsineffizienzen, die auch auf ihre distributiven und administrativen Folgen untersucht werden, ehe die Arbeit mit einer ökonomisch begründeten Empfehlung für die staatliche Informationssicherheitspolitik hinsichtlich offener Kommunikationsnetze und -dienste schließt.

Zum methodischen Vorgehen muß angemerkt werden, daß eine volkswirtschaftliche Effizienzanalyse nur auf einem gewissen Abstraktionsniveau durchgeführt werden kann. Zwar wird versucht, den grundsätzlichen Eigenschaften moderner Kommunikationssysteme Rechnung zu tragen, jedoch wird von Detailaspekten abstrahiert. Außerdem kann die Untersuchung in Ermangelung monetärer Daten sowohl der Nutzen- als auch der Kostenseite keine quantitativen, sondern nur qualitative Ergebnisse hervorbringen, die aber durchaus als Entscheidungsgrundlagen für den politischen Entscheidungsprozeß dienen können.

2.2 Ein Überblick über Kommunikationsnetze und -dienste

In dieser Arbeit werden Kommunikationsnetze generell als nachrichten- oder fernmeldetechnische Übertragungseinrichtungen verstanden, die den angeschlossenen Wirtschaftssubjekten erlauben, auf verschiedene Arten miteinander zu kommunizieren. Die für einen Kommunikationsprozeß notwendigen Bausteine lassen sich in Übertragungsnetze, bestehend aus Leitungen und Vermittlungsstellen bzw. Netzknoten, Teilnehmeranschlüsse und Endgeräte, unterteilen. Eine erfolgreiche Kommunikation zwischen zwei Teilnehmern verlangt zum einen eine Anschlußmöglichkeit der Endgeräte an die Netzanschlußstellen und zum anderen - analog zu einer gemeinsamen Sprache - einen einheitlich durchgeführten Kommunikationsprozeß, sogenannte Kommunikationsprotokolle. Zur Erläuterung kann hier das OSI-Modell (=„reference model for Open Systems Interconnection") allgemeiner Kommunikationsvorgänge angeführt werden, das von der internationalen Organisation für Standardisierung (ISO), der Dachorganisation der nationalen Normungsverbände, entwickelt wurde.[346] Grundlage einer jeden Kommunikationsbeziehung ist zunächst eine physische oder eine Funkverbindung zwischen den Netzanschlüssen der Teilnehmer, die die Übermittlung der Kommunikationsinhalte überhaupt erst ermöglicht. Auf diesen sogenannten Transportfunktionen bauen eine Reihe von Anwendungsfunktionen auf, die es letztlich auch erlauben, daß auf einer Basisverbindung unterschiedliche Kommunikationsprozesse bzw. -dienste ablaufen können. So werden Telefongespräche und Telefaxe auf denselben physischen Leitungen übermittelt, und in Mobilfunknetzen können in Zukunft neben Sprach- auch Dateninhalte mittels des Mobilfunkdienstes Modacom übertragen werden.[347] Dies bedeutet allgemein, daß auf den verschiedenen Netzen jeweils mehrere Kommunikationsdienstleistungen angeboten werden können. Die Begriffe Kommunikationsnetz und -dienst bzw. -dienstleistung werden deshalb im weiteren synonym gebraucht, weil letztere sowohl eines Kommunikationsnetzes bedürfen als auch aus ökonomischer Perspektive den Charakter von Netzgütern haben und in der Realität Kommunikationsdienste von Netzbetreibern oder von reinen Diensteanbietern offeriert werden.[348]

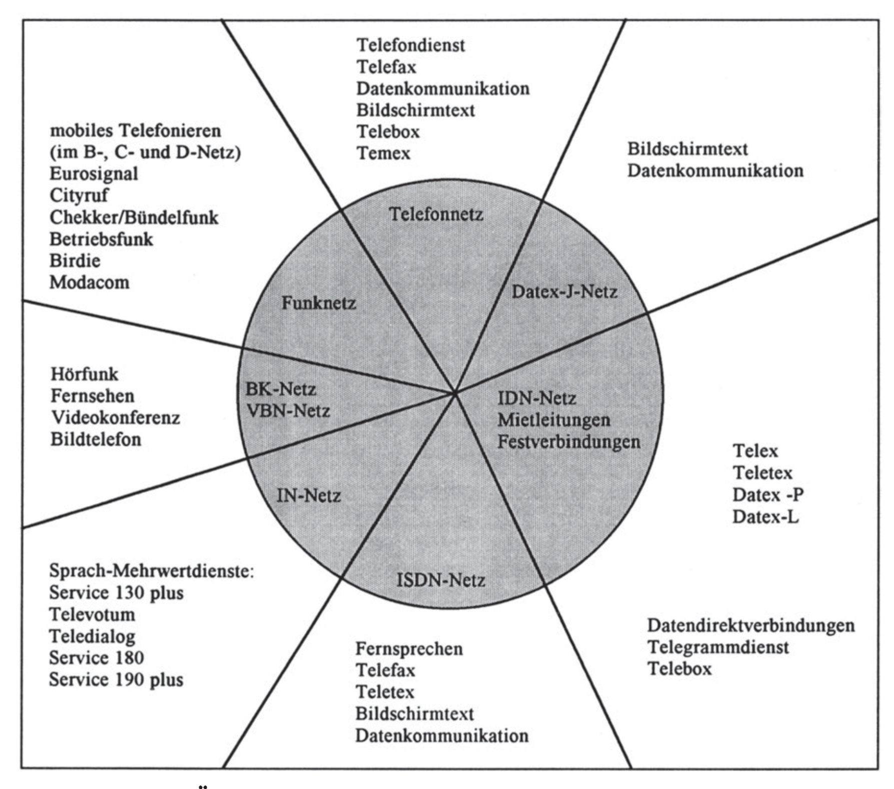
---

[346] Vgl. bzgl. einer genaueren Darstellung des OSI-Modells u. a. Franck (1986), S. 8-11, Gerke (1991), S. 204-210, und Welzel (1993), S. 7-10.

[347] Vgl. zu letzterem Fölling (1994).

[348] Vgl. dazu auch Hayashi (1993), S. 307.

Die folgende Darstellung gibt einen schemenhaften Überblick, welche Kommunikationsdienste (äußere Felder) auf welchen Festnetzen (innerer Kreis) in der Bundesrepublik Deutschland abgewickelt werden.[349]



Übersicht 5: Kommunikationsdienste und -netze

Im weiteren Vorgehen wird sich deshalb nicht speziell auf die Nachfrage nach Netzanschlüssen, sondern generell nach Kommunikationsdienstleistungen konzentriert. Diese umfassen neben der einfachen Sprachübertragung mittels Telefon auch sogenannte Mehrwertdienste.[350] Dazu zählen, wie auch Übersicht 5 zeigt, Online-

[349] Die Übersicht 5 entspricht Bild 1.3 von Ehlers (1994), S. 29, wobei BK für Breitband-Kommunikation, VBN für Vorläufer-Breitband-Netz, IN für intelligentes Netz, ISDN für Integrated Service Digital Network und IDN für integriertes Text- und Datennetz stehen. Vgl. zu den einzelnen Netzen und Diensten ebenda Kap. 2 bis 6.

[350] Vgl. zu einer Systematisierung Stoetzer (1991) und zur Übersicht der aktuellen Nutzungsintensität dieser Dienste in Stoetzer (1994).

Dienste[351], Videotext, E-Mail, elektronische Datenübertragungs- und Buchungssysteme und schließlich Sprach- und Videokonferenzen. Die folgende ökonomische Analyse der Informationssicherheit von Kommunikationssystemen beschränkt sich ausschließlich auf die echten „kommunikativen" Dienste, welche eine zweiseitige Kommunikation zwischen zwei Netzteilnehmern erlauben, so daß aus der Vielfalt der Mehrwertdienste Online-Dienste, Videotext und diejenigen Serviceleistungen keine Beachtung mehr finden, die lediglich eine einseitige Informationsversorgung der Teilnehmer leisten können und bei denen die Gesamtzahl der Nachfrager das Nutzenniveau eines repräsentativen Individuums nicht unmittelbar positiv beeinflußt.

Dieser Abschnitt sollte lediglich einen Überblick über die existierenden Kommunikationsmöglichkeiten in der Bundesrepublik bieten ohne detailliert auf die jeweiligen technischen Eigenschaften einzugehen, weil im weiteren Vorgehen ein Abstraktionsniveau gewählt wird, das zunächst eine mikroökonomische Modellierung der Netze und Dienste und schließlich eine darauf aufbauende Bestimmung des jeweils optimalen Informationssicherheitsniveaus ermöglicht.

---

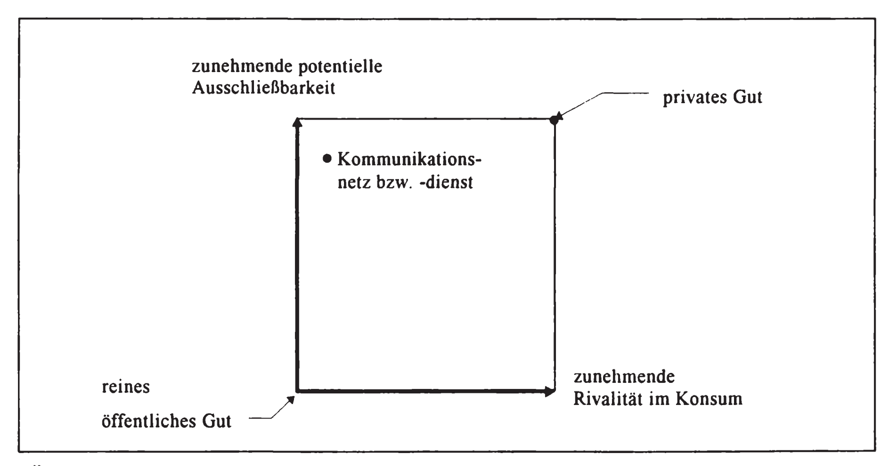
351 Vgl. zur aktuellen Situation der Online-Anbieter in Deutschland Borchers (1995).

2.3 Eine Charakterisierung von Kommunikationsnetzen und -diensten nach ökonomischen Kriterien

Von Seiten der ökonomischen Theorie existieren verschiedene Ansätze, Kommunikationsnetze bzw. -dienste zu beschreiben. Betrachtet man diese von der Kostenseite, dann zeichnen sie sich aufgrund der Einrichtung von Vermittlungsstellen und eines Verwaltungsapparates durch einen hohen Fixkostenblock und geringe Grenzkosten zusätzlicher Netzanschlüsse aus, so daß durch den Eintritt weiterer Teilnehmer die Durchschnittskosten gesenkt werden und sie damit den Charakter eines „cost sharing arrangement"[352] zwischen verschiedenen Wirtschaftssubjekten haben.[353] Ausgehend von der Nutzenseite läßt sich ein Kommunikationsdienst auch durch die Einordnung in die Dichotomie zwischen privatem und öffentlichem Gut definieren. Während ein privates Gut nur von einem Wirtschaftssubjekt konsumiert bzw. genutzt werden kann, zeichnen sich reine öffentliche Güter dadurch aus, daß alle Wirtschaftssubjekte sie gleichzeitig, ohne Überfüllungserscheinungen zu verursachen, nutzen können. Bei Kommunikationsnetzen bzw. -diensten liegt der Entstehungsgrund zwar gerade darin, daß mehrere Individuen sie simultan nutzen können und wollen, so daß sie keine privaten Güter sind. Jedoch erfüllen sie i. d. R. nicht die beiden strengen Bedingungen der Nichtrivalität im Konsum und der Nichtausschließbarkeit, weil zum einen die Leitungs- und Verwaltungskapazitäten der Betreiber von Kommunikationssystemen begrenzt sind und zum anderen durch die Erhebung von Benutzungsgebühren Zahlungsunwillige von der Nutzung ausgeschlossen werden können.[354] Dies sind aber die typischen Kennzeichen eines Clubgutes, welches in dem Spektrum zwischen öffentlichem und privatem Gut anzusiedeln ist, so daß sich zur ökonomischen Beschreibung von Kommunikationsnetzen die Clubgütertheorie anbietet.[355] Graphisch verdeutlicht Übersicht 6, in welcher eine Kategorisierung der verschiedenen Gutstypen nach den angegebenen Kriterien vorgenommen wird, die qualitative Position von Kommunikationsnetzen und -diensten. Schließlich handelt es sich bei den kosten- und nutzenseitigen Definitionen nicht um substitutive, sondern um komplementäre Ansätze, deren Verbindungsstücke die durch die meist gegebene Nichtrivalität im Konsum ermöglichte Teilung des Fixkostenblocks und die aufgrund unbedeutender Überfüllungserscheinungen zu vernachlässigenden variablen Kosten sind.

---

352 Noam (1992a), S. 111.
353 Vgl. genauer zur Kostenseite von Netzen Blankart & Knieps (1992), S. 74ff.
354 Vgl. dazu auch Liebowitz & Margolis (1994), S. 135f.
355 So sprechen z. B. Artle & Averous (1973), S. 91, von einem Telefonclub.



Übersicht 6: Kommunikationssysteme zwischen öffentlichen und privaten Gütern

In der nachfolgenden Untersuchung wird von Angebotsbeschränkungen von seiten der Netzbetreiber und Diensteanbieter abstrahiert, weil das Ziel nicht die Untersuchung des Marktes für Kommunikationsnetz- und -diensteanschlüsse, sondern lediglich eine für die Analyse der Informationssicherheitsproblematik geeignete Beschreibung verschiedener Netze und Dienste ist. Deshalb wird vereinfachend davon ausgegangen, daß es Gruppen von jeweils homogenen Kommunikationsteilnehmern auch möglich ist, die für sie optimalen „Kommunikationsclubs“ zu realisieren.

2.4 Die optimalen Größe-Leistungs-Kombinationen von Kommunikationsnetzen und -diensten

Bevor das effiziente Ausmaß an Informationssicherheit in verschiedenen Kommunikationsnetzen und -diensten bestimmt werden kann, müssen Kriterien ermittelt werden, welche sich zum einen dazu eignen, möglichst alle Kommunikationsnetze bzw. -dienste zu charakterisieren, und zum anderen eine adäquate Basis für die ökonomische Bestimmung der nutzenmaximierenden Netzeigenschaften bilden, welche schließlich die entscheidenden Determinanten bei der Ermittlung des effizienten Niveaus an Informationssicherheit sein werden.

Die üblichen technischen Kriterien zur Systematisierung der Vielfalt von Kommunikationsnetzen und -diensten sind Einteilungen in Fest- und Funknetze, nach ihrer Flächendeckung und Dichte, nach ihrer Kompatibilität, nach Einweg- oder Zweiweg-Interaktionen und nach ihrer Bandbreite bzw. Übertragungskapazität. Die ökonomische Analyse von Netzwerken hat sich vorwiegend auf die Anzahl der Netzteilnehmer als Variable gestützt, weil diese sowohl die Nutzen- als auch die Kostenseite eines Kommunikationsnetzes bzw. -dienstes maßgeblich bestimmt.[356] Dies ist für einfache Telefonnetze auch gerechtfertigt, jedoch machen es die zunehmende Leistungsfähigkeit der Kommunikationsnetze und die daraus resultierende Vielfalt der Dienstleistungen notwendig, dafür ein weiteres Kriterium, das die qualitativen Leistungsaspekte abbildet, einzuführen. Angeregt von der Entwicklung des ISDN[357], welches neben Sprach- auch Datenübertragung ermöglicht, ist es realitätsgetreuer und auch für die ökonomische Analyse operational, den Integrationsgrad I, d. h. den potentiellen Informationsübertragungsumfang bzw. die Leistungsfähigkeit, als weiteres Kriterium zur Charakterisierung von Kommunikationsnetzen und -diensten heranzuziehen, denn auch hier bestehen eindeutige Beziehungen sowohl zum individuellen Teilnehmernutzen als auch zu den entstehenden Gesamtkosten.[358]

Zwar können durch die Integration verschiedener Serviceleistungen sowohl Economies of Scope durch Bündelungsvorteile als auch Economies of Scale durch eine Ausdehnung des Teilnehmerkreises realisiert werden, so daß es aus Kostenge-

---

[356] Vgl. u. a. Artle & Averous (1973), Rohlfs (1974), Allen (1988) und Noam (1992), (1992a).

[357] Vgl. zur Ökonomie der Diensteintegration, Noam (1992), S. 350-359. Eine kritische Würdigung der wirtschaftlichen und gesellschaftlichen Implikationen von ISDN liefern Kubicek & Berger (1990).

[358] Der Integrationsgrad I stellt genauso wie die Sicherheit eine Qualitätsdimension dar. Um die Sicherheitsproblematik differenzierter betrachten zu können, ist es jedoch vorteilhaft, n und I als exogene Parameter anzunehmen und daraus das optimale Ausmaß an Sicherheit abzuleiten.

sichtspunkten erstrebenswert wäre, wenn schließlich nur noch ein allumfassender Kommunikationsdienst auf einem hoch integrierten Netz, an dem alle Nutzer teilnehmen, übrigbliebe. Neben der Kostenseite muß aber auch die Nutzenseite der verschiedenen Teilnehmeruntergruppen beachtet werden.[359] Denn es ist aufgrund heterogener Nachfragerpräferenzen volkswirtschaftlich effizient, wenn nebeneinander mehrere Netze und Dienste mit unterschiedlichem Leistungsumfang und verschiedenen Nutzergruppen bestehen[360], so daß auch in Zukunft eine gewisse Vielfalt existieren und die Kategorisierung nach Teilnehmerzahl und Integrationsgrad sich auch weiterhin als sinnvoll erweisen wird, wobei Netzübergänge nicht ausgeschlossen werden. Paradebeispiele dafür sind das Internet[361] oder die Verbindungen von Funk- und Festnetzen. In der theoretischen ökonomischen Analyse wird aber von der grundsätzlichen Netzübergangs- und der damit verbundenen Standardisierungsproblematik abgesehen, auf welche nur bei der Frage nach Externalitäten von Informationssicherheitsmaßnahmen eingegangen wird.[362]

Im Gegensatz zur traditionellen Netzwerkökonomie, welche sich im allgemeinen auf die Teilnehmerzahl als einzige Variable stützt, wird im folgenden deshalb von einer individuellen Nutzenfunktion U ausgegangen, in welche neben der Anzahl der potentiellen Kommunikationspartner n auch der Integrationsgrad I als qualitative Leistungsdimension des Kommunikationsnetzes bzw. -dienstes mit positivem Vorzeichen eingeht:

$$(27) \quad U = U(n, I).$$

Dabei haben die partiellen Ableitungen folgende Vorzeichen: $\partial U/\partial n>0$, $\partial^2 U/\partial n^2<0$, $\partial U/\partial I>0$ und $\partial^2 U/\partial I^2<0$.

Zunächst werden die optimalen Netzteilnehmerzahl bei gegebenem Integrationsgrad und der optimale Integrationsgrad bei gegebener Nutzerzahl mittels partieller

---

359 Vgl. allgemein zum volkswirtschaftlichen Trade-off zwischen der Ausschöpfung von Skalenerträgen und der Produktvielfalt Lancaster (1975).

360 Vgl. dazu Noam (1992), S. 356ff, und Mulgan (1991), S. 106. Kubicek (1991a), S. 55, argumentiert außerdem, daß eine diversifizierte Netzlandschaft analog zur Portfoliotheorie das Gesamtrisiko für die Gesellschaft senkt und deshalb eine vollständige Integration aller Netzdienste und aller Teilnehmer in ein Kommunikationsnetz nicht anzustreben sei.

361 Vgl. dazu u. a. Millin (1994).

362 Vgl. zur Ökonomie von Standards allgemein David & Greenstein (1990) und von Telekommunikationsstandards u. a. Besen & Saloner (1989).

Optimierung bestimmt.[363] Abschließend wird das Gesamtoptimum ermittelt. Die optimalen Kombinationen aus Netzgröße bzw. Nutzerzahl und Integrationsgrad eines Kommunikationsnetzes oder -dienstes werden dann dazu herangezogen, jeweils die nach ökonomischen Kriterien effiziente Informationssicherheit zu bestimmen.

2.4.1. Die Bestimmung der optimalen Teilnehmerzahl eines Kommunikationsnetzes oder -dienstes

Die Grundannahme des weiteren Vorgehens ist die Homogenität der betrachteten Kommunikationsteilnehmer, weil bei einer hinreichend großen Angebotsvielfalt sich jeweils Individuen mit ähnlichen Präferenzen und Eigenschaften dem Dienst anschließen werden, der ihren Bedürfnissen am nächsten kommt.[364] Zur Bestimmung der optimalen Teilnehmerzahl n* eines Kommunikationsnetzes wird zunächst sein Leistungsumfang bzw. sein Integrationsgrad I, welcher von allen Individuen im gleichen Maße genutzt wird, als gegeben angenommen. Anhand des folgenden individuellen Nutzenmaximierungskalküls wird die optimale Netzgröße n* bestimmt.[365]

Wie schon angedeutet, setzen sich die Gesamtkosten[366] eines Kommunikationsnetzes in Abhängigkeit von der Teilnehmerzahl n aus dem Fixkostenblock $F(\bar{I}) > 0$ und den teilnehmerabhängigen variablen Kosten f(n,I) zusammen:

$$(28) \quad TC(n,\bar{I}) = F(\bar{I}) + f(n,\bar{I})$$

mit $\partial f(n,\bar{I}) / \partial n > 0$ und $\partial^2 f(n,\bar{I}) / \partial n^2 > 0$.[367]

---

363 Vgl. zu diesem Vorgehen in der Clubgütertheorie originär Buchanan (1965) und Cornes & Sandler (1986), S. 164-169.

364 Vgl. dazu auch Noam (1992a), S. 123. Dies ist dasselbe Abstimmungsverhalten, das Tiebout (1956) den Wirtschaftssubjekten bzgl. der Wahl des Wohnortes bzw. der Ausstattung mit lokalen öffentlichen Gütern unterstellt.

365 Vgl. dazu Heal (1989), S. 5-12, und Noam (1992a), S. 111ff.

366 Die Kosten für einzelne Kommunikationsvorgänge und ihr Einfluß auf die Teilnahmeentscheidung des Individuums werden aufgrund ihrer in einem Wettbewerbsmarkt geringen Bedeutung vernachlässigt. Vgl. zu den Interdependenzen zwischen der Nachfrage nach „usage“ und „access“ Wenders (1987), Kapitel 3.

367 Die variablen Kosten nehmen demnach mit der Teilnehmerzahl n zu.

Der individuelle Nutzen aus der Mitgliedschaft an einem Kommunikationsnetz U sei eine positive Funktion der Gesamtteilnehmerzahl n. Es werden also positive Netzwerkexternalitäten unterstellt ($\partial U/\partial n>0$), wobei aber der Grenznutzen ($\partial^2 U/\partial n^2<0$) abnimmt.[368] Je mehr potentielle Gesprächs- bzw. Kommunikationspartner vorhanden sind, desto mehr Nutzen zieht das einzelne Wirtschaftssubjekt aus einem Anschluß an ein Kommunikationsnetz oder -dienst. Der abnehmende Grenznutzen kann dagegen dadurch begründet werden, daß das Interesse bezüglich zusätzlicher Kommunikationspartner abnimmt. Dies wird deutlich, wenn man davon ausgeht, daß sich diejenigen mit den stärksten Kommunikationspräferenzen zuerst zusammenschließen werden und die Kommunikationsintensität mit den dann hinzukommenden Teilnehmern geringer ist. Als Opportunitätskosten geht der Preis, den das Individuum für seinen Anschluß entrichten muß, mit negativem Vorzeichen in die Nutzenfunktion ein.[369] Außerdem wird unterstellt, daß der Nutzen in monetären Einheiten gemessen werden kann und daß die Nutzenfunktion bezüglich ihrer einzelnen Komponenten additiv ist. Deshalb gilt:

$$(29) \quad U(n,I,P) = -P(n,\bar{I}) + U(n,\bar{I}).$$

Schließlich wird davon ausgegangen, daß alle „Club-“ bzw. Netzteilnehmer den gleichen Anteil zur Bestreitung der Gesamtkosten aufbringen müssen[370], so daß der Preis P in Höhe der Durchschnittskosten $AC = \frac{1}{n} \cdot (F(\bar{I}) + f(n,\bar{I}))$ festgelegt wird, wobei i. d. R. wegen der sehr geringen Grenzkosten von einem fallenden Verlauf ausgegangen wird und die Durchschnittskosten erst bei sehr hohen Teilnehmerzahlen aufgrund von Überlastungen in nutzungsintensiven Zeiten wieder ansteigen. Sowohl die Durchschnittskostenkurve als auch die individuelle Nutzenfunktion

---

368 Man spricht hier auch von direkten Netzwerkexternalitäten im Gegensatz zu indirekten, welche auf keiner direkten physischen Verbindung basieren, sondern auf der Tatsache, daß eine Zunahme der Benutzer von (komplementären) Gütern wie Software deren Preis senkt und ihre Angebotsvielfalt erhöht. Vgl. dazu Katz & Shapiro (1985), S. 424.

369 Im Gegensatz zur Nutzenfunktion von Gleichung (27) wird hier schon die Budgetrestriktion integriert. Der Preis P(n,I) kann als Einbuße beim Bündel der übrigen Konsumgüter interpretiert werden. Die Gebühren für die Nutzung des Netzes werden vernachlässigt, da sie für die weitere Untersuchung keine Bedeutung haben.

370 Durch Wettbewerb zwischen Netz- und Diensteanbietern wird es zu einem Marktgleichgewicht in Form der monopolistischen Konkurrenz kommen, in welchem langfristig Netz- oder Dienstebetreiber trotz gewisser Monopolmacht keine positiven Gewinne realisieren werden. Vgl. dazu auch Liebowitz & Margolis (1994), S. 141ff. Auch Hayashi (1993), S. 301ff, geht davon aus, daß sich in Zukunft für alle Kommunikationsnetze und -dienste Wettbewerb durchsetzen wird.

werden in Abbildung 10 als Funktion der Anzahl der Kommunikationsteilnehmer n dargestellt, wobei der Integrationsgrad I als gegeben angenommen wird.[371]

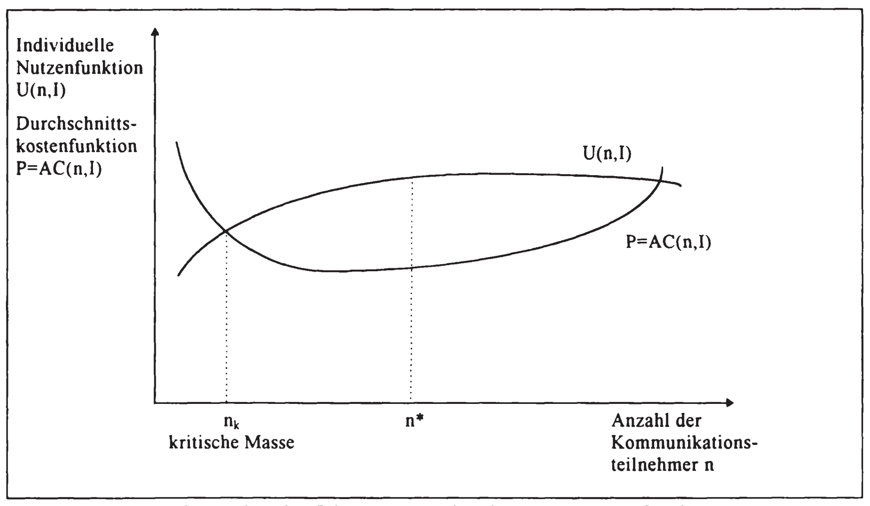


Abb. 10: Die optimale Teilnehmerzahl eines Kommunikationssystems

Vor der Bestimmung der optimalen Netzteilnehmerzahl n* muß zunächst kurz auf die Bedeutung der kritische Masse n_k eingegangen werden. Aufgrund der positiven Netzwerkexternalitäten zusätzlicher Netzteilnehmer und wegen der starken Degression der Durchschnittskosten bei geringen Teilnehmerzahlen wird sich ein Kommunikationsnetz nur in dem Fall langfristig durchsetzen, wenn eine gewisse kritische Masse n_k erreicht wird, weil die betrachteten Individuen nur dann einen Anreiz haben, sich an das Netz anschließen zu lassen[372] bzw. weil der Netzanbieter bzw. Clubbetreiber erst danach die Verlustzone verläßt und kostendeckend wirtschaften kann.[373]

Kann davon ausgegangen werden, daß der kritische Masse-Punkt überschritten ist, besteht nun die Intention darin, das private Optimum bezüglich der Netzgröße n zu

371 Vgl. eine ähnliche Abbildung in Noam (1992a), S. 113.

372 Vgl. dazu Noam (1992a), S. 112, oder Heal (1989), S. 6ff.

373 Vgl. dazu Allen (1988), S, 259. Vor dem Erreichen der kritischen Masse wird der Preis höchstens gleich der Zahlungsbereitschaft sein und damit unter den Durchschnittskosten liegen. Die Strategien zur Erreichung der kritischen Massen sind schon lange Zeit von großem Interesse, haben aber in diesem Abschnitt keine weitere Relevanz. Vgl. dazu u. a. Squire (1973), Rohlfs (1974), Oren & Smith (1981), Allen (1988) und Schoder (1995).

ermitteln.[374] Dazu ist die Nutzenfunktion von Gleichung (29) bezüglich n unter der Nebenbedingung P=AC zu maximieren. Dies führt zur Optimalitätsbedingung (30) bzw. nach einer Umformung zu (30′).[375]

$$(30) \quad \frac{dU}{dn} = -\frac{\partial AC(\bar{I})}{\partial n} + \frac{\partial U(\bar{I})}{\partial n} \overset{!}{=} 0$$

$$\text{bzw. } (30') \quad \frac{\partial U(n^*,\bar{I})}{\partial n^*} = \frac{f'(n^*,\bar{I})}{n^*} - \frac{AC(n^*,\bar{I})}{n^*}.$$

Im Nutzenoptimum bezüglich der privaten Teilnehmerzahl n* entspricht der marginale Anstieg des individuellen Nutzens durch einen weiteren Netzteilnehmer der Differenz von Grenz- und Durchschnittskosten pro Person.[376] Eine exakte Lösung von Gleichung (30′) ist im Rahmen dieser allgemeinen Modellierung nicht zu bestimmen, jedoch wird, wie in Abbildung 10 dargestellt, n* im aufsteigenden Ast der Durchschnittskostenkurve liegen. Haben sich n* Individuen gefunden, besteht unter der angenommenen Preisgestaltung kein Anreiz mehr, zusätzliche Teilnehmer aufzunehmen, weil dies die Summe der Nettonutzen bzw. der Konsumentenrenten aller Clubmitglieder reduziert. Es wird vereinfachend unterstellt, daß die n* Teilnehmer auch die Möglichkeit haben, weitere potentielle Nutzer auszuschließen.[377]

2.4.2 Die Bestimmung des optimalen Integrationsgrades eines Kommunikationsnetzes und -dienstes

Das Vorgehen zur Bestimmung des optimalen Integrationsgrades I* ist analog zur Ermittlung von n*. Es wird angenommen, daß die Teilnehmerzahl n gegeben ist.

---

374 Vgl. dazu Noam (1992a), S. 113f, oder genauer Heal (1989), S. 5ff.

375 Man kommt auf (30′), indem man $\partial AC/\partial n$ ausdifferenziert, denn es gilt: $\partial AC/\partial n = 1/n[f'(n) - AC]$.

376 Die Bedingung 2. Ordnung für ein Maximum ist dadurch erfüllt, daß n* im Bereich zunehmender Durchschnittskosten liegt.

377 Verläßt man die Clubbetrachtung von Kommunikationsnetzen, dann kann der Netzbetreiber trotz fehlendem Gewinnanreiz eine Expansion der Teilnehmerzahl über n* hinaus anstreben. Dies kann jedoch durch die Steigerung der Durchschnittskosten und der Heterogenität der Teilnehmergruppe zu Austritten der ursprünglichen Nutzer führen, wenn diese die Möglichkeit zum Aufbau eines neuen Netzes sehen, so daß sich auch langfristig eine Teilnehmerzahl nicht weit von n* einstellen wird. Vgl. dazu Noam (1992a), S. 116ff.

Die Gesamtkosten eines Kommunikationsnetzes sind eine Funktion des Integrationsgrades I:

$$(31)\ TC = F(I) + f(I,\bar{n}) \quad \text{mit}$$

$$\partial F(I)/\partial I > 0,\ \partial^2 F(I)/\partial I^2 > 0,\ \partial f(I,\bar{n})/\partial I > 0 \text{ und } \partial^2 f(I,\bar{n})/\partial I^2 > 0.$$

Der Preis P, den ein Individuum für die Nutzung eines Kommunikationsnetzes mit dem Integrationsgrad I bezahlen muß, ist gleich den Durchschnittskosten $AC = \frac{1}{\bar{n}} \cdot (F(I) + f(I,\bar{n}))$. Der Gesamtnutzen eines Individuums, den es aus dem Leistungsumfang I zieht, wird in Gleichung (32) deshalb wie folgt bestimmt:

$$(32)\ U(P,n,I) = -P(I,\bar{n}) + U(I,\bar{n}).$$

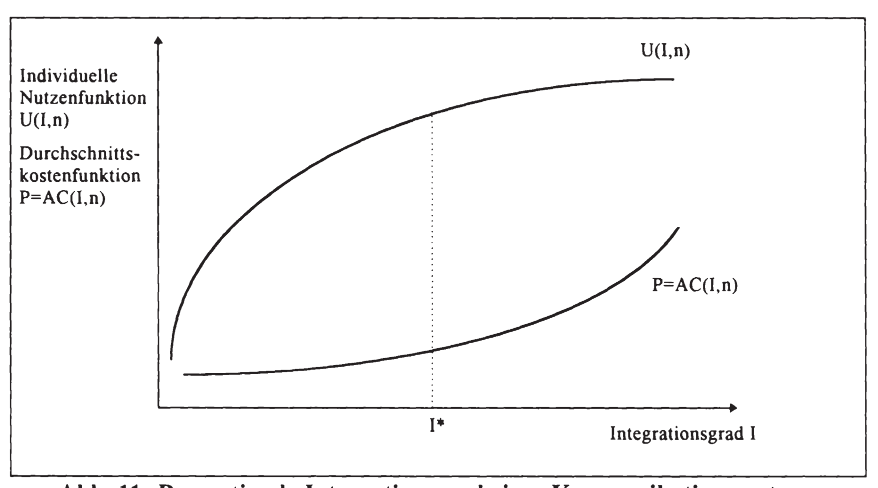


Abb. 11: Der optimale Integrationsgrad eines Kommunikationssystems

Der individuelle Grenznutzen eines höheren Leistungsumfangs I ist zwar positiv ($\partial U/\partial I > 0$), nimmt aber entsprechend dem ersten Gossenschen Gesetz ab ($\partial^2 U/\partial I^2 < 0$). In Abbildung 11 werden sowohl die individuelle Nutzenfunktion als auch die Durchschnittskostenfunktion in Abhängigkeit vom Integrationsgrad I abgetragen.[378]

---

[378] Neben der kritischen Masse von Teilnehmern wird inzwischen auch eine kritische Masse von Dienstleistungen diskutiert, die erreicht werden muß, damit sich eine neue Kommunikationstechnik

Zur Bestimmung des Optimums I* muß die Nutzenfunktion aus Gleichung (32) bezüglich I maximiert werden. Daraus folgt die Optimalitätsbedingung (33) bzw. (33´):

$$(33)\quad \frac{dU}{dI} = -\frac{\partial AC}{\partial I} + \frac{\partial U(I,\bar{n})}{\partial I} \overset{!}{=} 0$$

$$\text{bzw. } (33')\quad \frac{\partial U(I^*,\bar{n})}{\partial I^*} = \frac{1}{\bar{n}}\left[\frac{\partial F(I^*,\bar{n})}{\partial I^*} + \frac{\partial f(I^*,\bar{n})}{\partial I^*}\right].$$ [379]

Im Optimum muß der Grenznutzen des Integrationsgrades I* den vom Individuum aufzubringenden Grenzkosten entsprechen.[380]

2.4.3 Die Bestimmung eines simultanen Optimums des Integrationsgrades und der Teilnehmerzahl

In den vorangegangenen Abschnitten wurden die Optima von n* und I* bei Exogenität des jeweils anderen Parameters bestimmt. Zur Bestimmung des simultanen Optimums (n*, I*) wird aus Anschaulichkeitsgründen auf eine formale Herleitung verzichtet und eine rein graphische Darstellung gewählt.[381]

Das absolute Wohlfahrtsmaximum zeichnet sich dadurch aus, daß die beiden Bedingungen (30´) und (33´) simultan erfüllt sind, so daß gilt:

$$(30'')\quad \frac{\partial U(n^*,I^*)}{\partial n^*} = \frac{f'(n^*,I^*)}{n^*} - \frac{AC(n^*,I^*)}{n^*}$$

$$\text{und } (33'')\quad \frac{\partial U(I^*,n^*)}{\partial I^*} = \frac{1}{n^*}\left[\frac{\partial F(I^*,n^*)}{\partial I^*} + \frac{\partial f(I^*,n^*)}{\partial I^*}\right].$$

durchsetzt. Dieser Gesichtspunkt wird hier aber nicht weiter verfolgt. Vgl. dazu Castelli & Leporelli (1993).

379 Man kommt auf (33´), indem man dAC/dI ausdifferenziert, denn es gilt: $\partial AC/\partial I = 1/n[\partial F(I,n)/\partial I + \partial f(I,n)/\partial I]$. Die Bedingung 2. Ordnung für ein Maximum ist durch die Konkavität der Nutzenfunktion und die Konvexität der Kostenfunktion erfüllt.

380 Gleichung (33´) entspricht multipliziert mit n der Samuelson Bedingung für die Erstellung von öffentlichen Gütern, nach welcher die Summe der Grenznutzen gleich den Grenzkosten sein muß.

381 Vgl. dazu u. a. Buchanan (1965), Berglas (1976), S. 116f, und Cornes & Sandler (1986), S. 168f.

Graphisch läßt sich dies an Abbildung 12 verdeutlichen, wobei die Funktion n*(I) aus der Optimalitätsbedingung von Gleichung (30′) und die Funktion I*(n) aus (33′) durch Änderung des jeweils exogenen Parameters abgeleitet werden. Das Totaloptimum ist durch den Schnittpunkt der beiden Kurven definiert.[382]

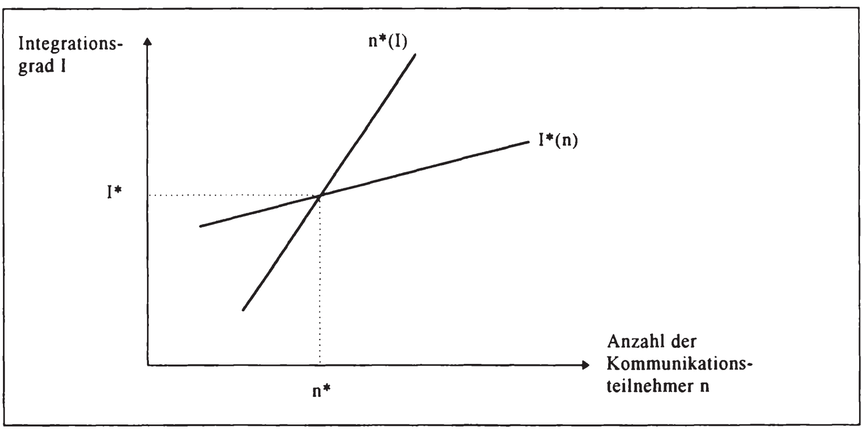


Abb. 12: Simultanes Optimum von Teilnehmerzahl und Integrationsgrad

Unterstellt man eine homogene Gruppe von Kommunikationsteilnehmern mit der in Gleichung (27) unterstellten Nutzenfunktion, dann ergibt die Maximierung der individuellen Nutzenfunktionen bei der unterstellten Preisbildung (P=AC) eine optimale Kombination von Teilnehmerzahl n* und Integrationsgrad I*, die das von diesen Individuen gewählte Kommunikationssystem beschreibt, wobei von Restriktionen der Angebotsseite abstrahiert wird. Denn sowohl die Deregulierung des Telekommunikationssektors als auch die Weiterentwicklung der Telekommunikationstechnik können eine vielfältige Angebotsstruktur entstehen lassen, die den einzelnen Individuen die Möglichkeit eröffnet, ein Kommunikationsnetz zu wählen, das ihrer optimalen Kombination von n* und I* schon sehr nahe kommt. Entsprechend dem Optimierungsverhalten der betrachteten Gruppe werden sich andere Telefonclubs mit einer homogenen Teilnehmergruppe bilden, so daß weitere n*-I*-Kombinationen entstehen können.[383] Die folgende Abbildung 13 macht dies deutlich. Die Kombination $A(n_3^*, I_3^*)$ stellt ein sehr leistungsfähiges Kommunika-

---

382 Damit es sich um ein Maximum handelt, wird zusätzlich zu $\partial^2U/\partial n^2<0$ und $\partial^2U/\partial I^2<0$ unterstellt, daß das Produkt der zweiten partiellen Ableitungen $[(\partial^2U/\partial n^2)(\partial^2U/\partial I^2)]$ größer ist als $[\partial^2U/\partial n\partial I]^2$. Vgl. dazu Chiang (1984), S. 317.

383 Graphisch ausgedrückt wählt ein Individuum in der n-I-Ebene aus dem Angebot der Kommunikationsnetze und -dienste dasjenige aus, das seiner am stärksten präferierten n*-I*-Kombination am nächsten kommt.

tionssystem mit einem kleinen Teilnehmerkreis dar, während die Kombination $B(n_1^*, I_1^*)$ von einer breiteren Gruppe nachgefragt wird und es sich bei $C(n_2^*, I_2^*)$ um einen typischen Massenkommunikationsdienst, wie z. B. um das Telefon handelt. Da die Bedürfnisse mancher Individuen sowohl hinsichtlich Teilnehmerzahl als auch Leistungsvermögen durch ein Kommunikationsnetz oder -dienst nur unvollständig befriedigt werden, können gleichzeitig auch mehrere verschiedene Kommunikationsanschlüsse, wie zu Fest- und Mobilfunknetzen[384], oder solche Kommunikationssysteme gewählt werden, die durch eine ausreichende Kompatibilität der Kommunikationsprotokolle auch ein Zusammenschalten mit anderen Netzen erlauben, wie es beim Verbinden von inländischen mit ausländischen Telefonnetzen der Fall ist.[385]

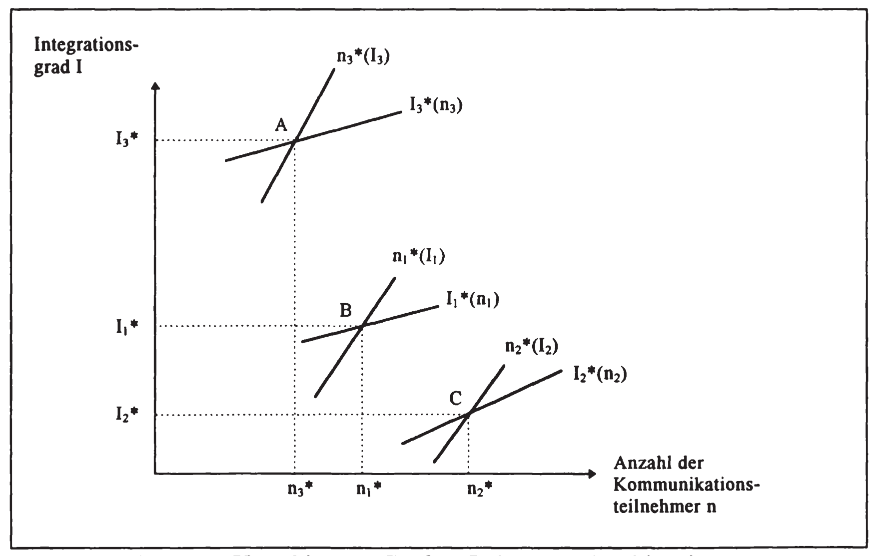


Abb. 13: Verschiedene Größen-Leistungs-Kombinationen von Kommunikationsnetzen und -diensten

Da sich die Telekommunikationsbranche gegenwärtig sowohl durch quantitative Expansion als auch durch qualitativen technischen Fortschritt auszeichnet, werden in der n-I-Ebene die Kommunikationssysteme zu höheren Teilnehmerzahlen und umfangreicheren Leistungsfähigkeiten expandieren.

---

384 So sollen bis zur Jahrtausendwende fast 25% der Teilnehmer des Festnetzes auch einen Mobilfunkanschluß besitzen. Vgl. Gronert (1995).

385 Vgl. dazu u. a. Mitchell & Vogelsang (1994) und Vogelsang (1995).

Ausgehend von den Parameterkombinationen (n*, I*) wird im folgenden Abschnitt versucht werden, nach der Erwartungsnutzentheorie die optimalen Informationssicherheitsniveaus in Kommunikationssystemen mit verschiedenen n*-I*-Kombinationen abzuleiten.

2.5 Eine ökonomische Analyse der Informationssicherheit in Kommunikationsnetzen und -diensten

2.5.1. Die teilnehmerspezifischen Gefahren und Risiken von Kommunikationsnetzen und -diensten

Bevor die Risiken, welche Kommunikationsvorgängen in Kommunikationssystemen drohen, aufgezeigt werden, muß zunächst genauer definiert werden, worum es sich bei einer Kommunikationsdienstleistung handelt. Ganz allgemein ist ein Kommunikationsvorgang nichts anderes als der Transport vielfältiger Informationen von einem Teilnehmer zu einem oder mehreren anderen Teilnehmern, den die Kommunikationssysteme mittels Sprach-, Daten- oder Bildübertragung zu leisten vermögen. Analog dazu transportieren z. B. Eisenbahnen auf ihren Schienennetzen Personen und Güter von einem Ort zum anderen.[386]

Bei dem transportierten Gut handelt es sich also um Informationen[387], die ohne definierte Eigentumsrechte[388] die Eigenschaften eines öffentlichen Gutes haben, weil durch die nahezu kostenlose Mitnutzung weiterer Individuen Nicht-Rivalität im Konsum gegeben ist. Durch die Übermittlung werden die Eigentumsrechte des Senders und in vielen Fällen auch des Empfängers an den Informationen unmittelbar bedroht.[389] Denn sowohl der Totalverlust der Informationsinhalte als auch die vielfältigen noch zu zeigenden Verletzungen der Eigentumsrechte verursachen i. d. R. einen Wohlfahrtsverlust bei den betroffenen Individuen, weil ihre Wertschätzung der Informationsübertragung sinkt oder sich der Gutscharakter der Informationen sogar in ein Übel verwandelt, wenn diese anderen Wirtschaftssubjekten bekannt werden.[390] Aus diesem Bedrohungspotential leitet sich schließlich eine posi-

---

[386] Vgl. zu einem Vergleich verschiedener Netzwerke und denen auf ihnen transportierten Objekten Hayashi (1993), S. 306.

[387] Eine Differenzierung des Begriffes Information nach ökonomischen Kriterien liefern u. a. Hirshleifer & Riley (1992), S. 167-170.

[388] Eigentumsrechte für Informationen und Kenntnisse werden hier in einem weiteren Sinne verstanden als diejenigen an materiellen Wirtschaftsgütern, weil sie auch nicht-kommerzielle Werte, wie das Bedürfnis nach einer geschützten Privatsphäre enthalten.

[389] Es gibt auch Informationsinhalte, wie Produktwerbung, die gerade an Wert gewinnen, wenn sie weit verbreitet werden. Vgl. dazu Mulgan (1991), S. 120. Diese werden aber nur bedingt in „kommunikativen" Netzen verbreitet.

[390] Im Gegensatz zu den ursprünglichen Transportsystemen geht es bei Kommunikationssystemen nicht um die materielle Unversehrtheit der Transportgüter, sondern vor allem um die Nichtverletzung von Eigentums- und Persönlichkeitsrechten.

tive Zahlungsbereitschaft für Informationssicherheit ab, die zur Implementierung von Informationssicherheitsmechnismen in Kommunikationssystemen führt.

Neben den Gefahren für die Informationssicherheit im Rahmen eines Kommunikationsprozesses ist vor allem der Datenschutz i. e. S. bzw. das Grundrecht auf informationelle Selbstbestimmung im Blickpunkt der öffentlichen Diskussion.[391] Im Kontext der Kommunikationsnetze und -dienste geht es vor allem um die Schutzwürdigkeit der sogenannten Verbindungsdaten von Kommunikationsverbindungen, welche umfassen, wer wann mit wem auf welchem Wege in welchem Ausmaß kommuniziert und damit personenbezogene Daten sind. Mit dem Wegfall der staatlichen Telekommunikationsmonopole und den erweiterten Möglichkeiten der elektronischen Datenverarbeitung müssen diese nun auch vor dem Zugriff nicht-öffentlicher Stellen geschützt werden, während in der Vergangenheit ausschließlich der Persönlichkeitsschutz des Bürgers gegenüber staatlichen Institutionen im Vordergrund stand. Die bei Kommunikationsprozessen anfallenden personenbezogenen Daten können zur Bildung eines Persönlichkeitsprofils herangezogen, zweckentfremdet und schließlich zur Verhaltenskontrolle verwendet werden.[392] Diese dem Datenschutz i. e. S. zuzuordnenden Gesichtspunkte stehen nicht im Mittelpunkt der Analyse, sondern es wird sich auf die Datensicherheit bzw. auf die noch genauer zu definierende Informationssicherheit der Kommunikationsinhalte beschränkt.[393] Denn der Datenschutz ist wegen seiner gesellschaftspolitischen Bedeutung durch die gesetzlichen Rahmenbedingungen in Form des Bundesdatenschutzgesetzes (BDSG) im allgemeinen und für den Telekommunikationssektor bereichsspezifisch in den Datenschutzverordnungen für die Deutsche Bundespost Telekom (TDSV) und für die sonstigen telekommunikationsdienstleistungserbringende Unternehmen (UDSV) geregelt. Außerdem steht der Datenschutz potentiell in einer Konfliktbeziehung zum Verbraucherschutz im Bereich der Kommunikationssysteme, weil die Abrechnungssicherheit der in Anspruch genommenen Kommunikationsdienstleistungen eine Speicherung der Verbindungsdaten i. d. R. voraussetzt. Schließlich ist die effizienteste Möglichkeit des Datenschutzes in diesem Kontext die Vermeidung bzw. unmittelbare Löschung persönlichkeitsbezogener Verbindungsdaten. Diese Gesichtspunkte machen den Datenschutz zu einem gesell-

---

391 Es handelt sich hier nicht um ein explizit formuliertes Grundrecht, sondern es wurde im Rahmen des „Volkszählungsurteils" durch das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitet. Vgl. dazu Vogelgesang (1987).

392 Vgl. dazu Garstka (1993), S. 32f.

393 Vgl. zu dieser Differenzierung u. a. Katz (1991), S. 58-68, und Büllesbach (1995), S. 4f. Dagegen versteht Pfitzmann (1993), S. 452, unter seinen Datenschutzanforderungen in öffentlichen Funknetzen sowohl Aspekte des Datenschutzes i .e. S. als auch Datensicherheit.

schaftspolitischen Thema und für die folgende ökonomische Analyse wenig geeignet. Jedoch fällt der Datenschutz beim Übermitteln personenbezogener Daten unter den Begriff der Datensicherheit.[394] Die Datensicherheit bzw. die noch detaillierter zu bestimmende Informationssicherheit werden Gegenstand der folgenden ökonomischen Analyse sein.

Zwar sind die allgemeinen Gefahren für Informationen während der Übermittlung in einem offenen Kommunikationssystem eingangs dieses Abschnittes schon angesprochen worden, jedoch ist eine präzisere Definiton der Informationssicherheit für das weitere Vorgehen und die Abgrenzung gegenüber dem Datenschutz i. e. S. angebracht. Unter Informationssicherheit wird in dieser Arbeit ein Zustand verstanden, in welchem eine Kommunikationsverbindung folgende Eigenschaften aufweist.[395] Erstens ist die Verfügbarkeit der zu übermittelnden Informationen durch das Funktionieren des Kommunikationssystems für Sender und Empfänger gewährleistet. Zweitens sind die Inhalte vor Verfälschung (=Integrität) und drittens vor unerwünschtem Bekanntwerden (=Vertraulichkeit[396]) geschützt. Schließlich kann den jeweiligen Sendern die Übermittlung von Kommunikationsinhalten fehlerfrei zugerechnet werden (=Authentizität), so daß vor allem Kommunikationsinhalte, die Vertragscharakter haben und materielle Transaktionen nach sich ziehen, unabstreitbar werden.[397]

Nach der Bestimmung des Begriffes Informationssicherheit durch seine verschiedenen Teilaspekte muß noch auf die Abgrenzungsmöglichkeiten anhand der potentiellen Gefährdungsquellen der Informationssicherheit in Kommunikationsnetzen eingegangen werden.[398] Dabei wird der Sicherheitsbegriff so umfassend gewählt, daß sowohl die klassischen Safety-Aspekte, welche sich auf die technische Sicherheit gegen die Bedrohung durch Unfälle beziehen, worunter man Übertragungsfehler, Ausfälle, Fehleranfälligkeit und Unzuverlässigkeit bzw. allgemein technisches und menschliches Versagen versteht, als auch die Security-Dimensionen inbegriffen sind, die die Sicherheit gegen Bedrohungen durch beabsichtigte Angriffe be-

---

394 Vgl. dazu Büllesbach (1995), S. 4.

395 Vgl. dazu Fumy & Riess, (1993), S. 118. Dieser Katalog von Sicherheitseigenschaften wird in der Informationstechnik auch international verwendet. Vgl. dazu auch das System Security Study Committee u. a. (1991), Kap. 2.

396 Einen komplexeren und Datenschutzaspekte integrierenden Vertraulichkeitsbegriff, der auch die Unbeobachtbarkeit und die Anonymität des eigentlichen Kommunikationsvorganges umfaßt, verwendet Rihaczek (1994), S. 512.

397 Pohl & Weck (1993a), S. 16, sprechen auch von „communication security“.

398 Vgl. zu dieser Begriffsdiskussion Pohl & Weck (1993), S. 19ff.

schreiben.[399] Denn eine strenge Unterscheidung zwischen Safety und Security ist in vielen Fällen nicht möglich und für die allgemeine ökonomische Analyse nicht hilfreich, da unabhängig davon, ob ein Schadensfall nun unter dem Safety- oder dem Security-Begriff einzuordnen ist, für die Betroffenen immer einen Wohlfahrtsverlust entsteht.[400]

Neben der Aufgabe der Differenzierung von Safety- und Security-Risiken wird auch auf die Dimensionen des Begriffes der mehrseitigen Sicherheit[401] verzichtet, welcher die gleichwertige Berücksichtigung der Interessen aller beteiligten Gruppen, nämlich der Hersteller der Kommunikationstechnik, den Betreibern von Netzen und Diensten, ihren Benutzern und den indirekt Betroffenen fordert. Denn die Realisierung mehrseitiger Sicherheit wird in der Realität lediglich für die Benutzer und die indirekt Betroffenen ein Problem darstellen, weil diese im Zweifel ihre Interessen gegenüber der Angebotsseite nicht durchsetzen werden. Denn sowohl die Hersteller als auch die Betreiber werden nur dann Kommunikationseinrichtungen und -dienste anbieten, wenn ihre Bedürfnisse, d. h. die korrekte Abrechnung und Bezahlung ihrer erbrachten Leistungen, erfüllt werden.[402] Da sie sich sowohl bezüglich der Kenntnisse über die Informationssicherheit als auch finanziell in der stärkeren Position befinden, werden sie ihre „Sicherheitsbedürfnisse“ zumindest langfristig durchsetzen. Fehlallokationen werden daher primär von den Unzulänglichkeiten der Nachfrageseite herrühren, die es mittels verschiedener staatlicher Instrumente zu beheben gilt.[403]

Nachdem sowohl die Risiken von Kommunikationsvorgängen in offenen Kommunikationssystemen in Form des potentiellen Verlustes der Verfügbarkeit, der Integrität und der Vertraulichkeit der Kommunikationsinhalte und der fehlerhaften Identifikation der Kommunikationsteilnehmer identifiziert werden als auch der

[399] In der weiteren Untersuchung wird von einem gegebenen rechtlichen Rahmen und konstanten Anstrengungen bzgl. der Prävention und der Verfolgung von Computerkriminalität unterstellt. Denn auf eine ökonomische Analyse der Strafverfolgung bzw. des Strafrechts als Instrument zur Verhinderung krimineller Aktivitäten wird verzichtet. Vgl. zu aktuellen Deliktsformen und zur Reaktion der Gesetzgeber Sieber (1995).

[400] Vgl. dazu auch Pohl & Weck (1993), S. 20. Dagegen versteht Müller (1994a), S. 2, unter „information security“ den Schutz der verarbeiteten Informationen sowohl vor absichtlichen als auch vor unbeabsichtigten Bedrohungen.

[401] Vgl. dazu Müller (1994) S. 3.

[402] Die fehlerhafte Abrechnung von Kommunikationsdienstleistungen geht meist zu Lasten der Teilnehmer. Vgl. Weishaupt (1994). Nur in Ausnahmefällen oder bei innovativen Diensten, wie dem Mobilfunk, können sich auch Teilnehmer auf Kosten der Betreibergesellschaften bereichern. Vgl. dazu o. V. (1994).

[403] Vgl. dazu die Abschnitte 2.6 und 2.7.

tangierte Personenkreis auf die Benutzer und auf die mit den Kommunikationsinhalten in Verbindungen zu bringenden Betroffenen beschränkt werden konnte, bedarf es nun einer Untersuchung der ökonomischen Implikationen von Verletzungen der Informationssicherheit in Kommunikationssystemen.

2.5.2 Eine nutzentheoretische Systematisierung der Risiken der Informationssicherheit in Kommunikationsnetzen und -diensten

Im Gegensatz zur Transportsicherheit im Verkehr, worunter man die unversehrte Beförderung von Gütern und Personen versteht, bezieht sich die Informationssicherheit in Kommunikationsnetzen auf den unversehrten Transport von Informationen und deshalb auch, wie in Abschnitt 2.5.1 aufgezeigt, auf den Schutz vor einer Vielzahl unterschiedlicher Risiken. Deshalb stellt die Bewertung der Schadenpotentiale, welche schon bei der Evaluierung der Straßenverkehrssicherheit[404] erhebliche Schwierigkeiten bereitet, ein besonderen Problemkreis dar.[405] Obwohl es sich bei Kommunikationsinhalten im Gegensatz zu den auf Straße, Schiene oder Luftweg transportierten Waren um keine materiellen Güter, sondern um immaterielle Informationen handelt, wird auch deren unversehrtem Transport ein positiver Nutzen bzw. ein monetärer Wert beigemessen. Im folgenden wird eine einfache qualitative Systematisierung der Kommunikationsrisiken hinsichtlich ihrer Auswirkungen auf die individuelle Vermögens- und Nutzensituation der Kommunikationsteilnehmer versucht, welche mit der im nächsten Abschnitt durchgeführten Analyse der Kosten von Informationssicherheitsmechanismen in Kommunikationssystemen die Basis für die Bestimmung des optimalen Informationssicherheitsniveaus bilden wird.

Die Nicht-Gewährleistung der geforderten Eigenschaften der Informationssicherheit bei Kommunikationsvorgängen kann zu Schadensfällen führen, die zwei qualitativ unterschiedliche Komponenten von negativen Beeinträchtigungen beinhalten. Die erste Komponente umfaßt den materiellen bzw. monetären Schaden, der in einem solchen Schadensfall auftritt. Im ersten Teil der Arbeit wird dahingehend argumentiert, daß der Schadenumfang ausschließlich durch eine monetäre Größe L ausgedrückt wird. Es wird davon abgesehen, daß bei Schadensfällen auch immaterielles Leid auftritt, das nicht durch monetäre Größen bzw. durch Marktpreise

404 Vgl. dazu u. a. Jones-Lee (1990), S. 40ff.

405 So spricht auch Moser (1995), S. 5, von „nicht leicht tangibel" zu machenden Größen.

quantifiziert werden kann. Diese Vorgehensweise ist jedoch nicht in Schadensfällen adäquat, wo allgemein akzeptierte Persönlichkeitsrechte und das psychische Wohlbefinden von Individuen beeinträchtigt wird. Bei Kommunikationsvorgängen spielen aber gerade diese Elemente neben den monetär bewertbaren Folgen von Eigentumsverletzungen hinsichtlich der Kommunikationsinhalte eine wesentliche Rolle, so daß auch sie in die theoretische ökonomische Analyse einfließen müssen. Die Nutzeneinbußen, die durch den Verlust immaterieller bzw. ideeller Werte verursacht werden, bilden deshalb die zweite Schadenskomponente.

Die folgende Abbildung 14 verdeutlicht, welchen qualitativen Unterschied es macht, ob bei einem Schadensfall nur ein materieller Schaden eintritt oder ob lediglich das seelische Wohlbefinden in Mitleidenschaft gezogen wird bzw. eine Persönlichkeitsrechtsverletzung vorliegt.

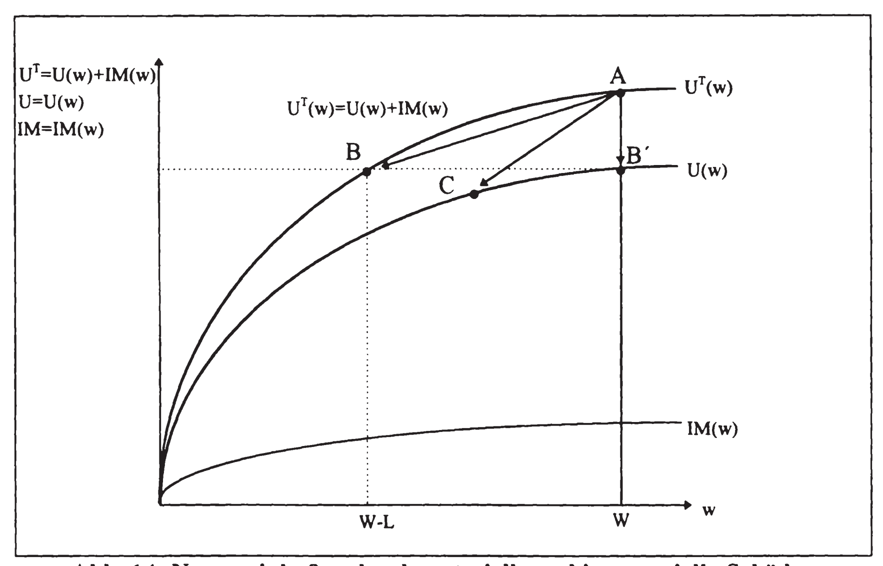


Abb. 14: Nutzeneinbußen durch materielle und immaterielle Schäden

Im ersten Fall sieht sich das Individuum dem bekannten Szenario gegenüber, in welchem es mit einer Wahrscheinlichkeit (1-p) im Ausgangspunkt A bleibt, während es mit der Schadenswahrscheinlichkeit p einen monetären Vermögensverlust L erleidet, der es auf Punkt B abrutschen läßt. Demgegenüber wird es bei einer reinen seelischen Beeinträchtigung zwar keinen Vermögensverlust erleiden, aber auf eine tiefer gelegene Nutzenfunktion U fallen, die sich gegenüber der ursprünglichen Nutzenfunktion U^T dadurch auszeichnet, daß das seelische Wohlbefinden,

ausgedrückt durch den ideellen Wert IM, negativ beeinträchtigt wird.[406] Dieser ideelle Wert kann in diesem Kontext die Gewährleistung der Vertraulichkeit der Inhalte privater Telefongespräche, deren Bekanntwerden für die Betroffenen jedoch keinerlei Vermögenseinbußen nach sich ziehen, darstellen. Es ist also deutlich geworden, daß analog zur Aufteilung des Gesamtschadens in eine materielle und in eine immaterielle Komponente auch die ursprüngliche Nutzenfunktion U^T in eine rein materielle Dimension U(w) und in einen ideellen Teilaspekt IM(w) aufgespalten werden muß, wobei letzterer im Schaubild zunächst positiv von der Vermögensposition abhängt. In der Realität werden Schadensfälle beide Schadenkomponenten, wie in Abbildung 14 durch den Punkt C dargestellt, aufweisen. Davon wird in der theoretischen Analyse, die lediglich einen Vergleich beider Konstellationen betrachtet, jedoch abstrahiert, weil dieses komplexere Entscheidungsproblem keinen zusätzlichen Erkenntnisgewinn einbringt.

In der Realität fallen unter die materielle Schadenkomponente alle Kosten, die entstehen, um verlorengegangene oder veränderte Kommunikationsinhalte wiederherzustellen, und diejenigen finanziellen Einbußen, welche durch die unzulängliche Vertraulichkeit von Kommunikationsbeziehungen und -inhalten hervorgerufen werden. So kann das Bekanntwerden sensibler Unternehmensdaten dazu führen, daß die Betroffenen erhebliche materielle Verluste erleiden, weil konkurrierende Unternehmen Kunden abwerben oder sich die Ergebnisse fremder Forschungsaktivitäten aneignen und verwenden. Ähnlich verhält es sich in Fällen, in denen es nicht immer gewährleistet ist, ob die angegebene Identität der Kommunikationspartner mit der wahren übereinstimmt, so daß Unbefugte über Kommunikationsprozesse andere Kommunikationspartner schädigen und sich bereichern können. Hierunter fallen z. B. Manipulationen von Kontoständen bei Kreditinstituten.

Bei einer Vielzahl von Kommunikationsvorgängen werden jedoch Inhalte übermittelt, deren Beeinträchtigung nicht zu materiellen und monetären Verlusten führen, weil sie für die Kommunizierenden nicht unmittelbar in einem kommerziellen Zusammenhang stehen. Dann ist die Sicherstellung eines vertraulichen Kommunikationsaktes als Erhöhung der Lebensqualität bzw. als fester Bestandteil der Persön-

[406] Diese Vorgehensweise stellt eine sogenannte „state-dependent utility function" dar. Vgl. dazu Hirshleifer & Riley (1992), S. 60ff.

lichkeitsrechte zu betrachten und stellt damit einen sogenannten intangiblen oder gar unersetzbaren Wert dar.[407]

Obwohl eine Bewertung der zweiten Schadenkomponente in monetären Einheiten nicht unmittelbar möglich ist, existieren Methoden zur Quantifizierung von Zahlungsbereitschaften, welche vor allem zur Bestimmung der Präferenzen für öffentliche Güter herangezogen werden.[408] Diese Verfahren können in direkte Methoden, welche über direkte Befragungen[409] oder Experimente die Zahlungsbereitschaft ermitteln, und in indirekte Methoden, die durch die Analyse beobachtbarer, interdependenter wirtschaftlicher Aktivitäten auf die Wertschätzung zu schließen versuchen, eingeteilt werden. Letzterer Ansatz, der sowohl auf Substitutions- als auch Komplementaritätsbeziehungen zurückgreifen muß, ist hinsichtlich der Informationssicherheit in offenen Kommunikationssystemen wenig vielversprechend, weil sowohl die Vielfalt an möglichen Informationssicherheitsstufen aufgrund einer gegenwärtig noch beschränkten Zahl von Netz- und Diensteanbietern gering ist[410] als auch das theoretisch mögliche Substitut - der Versicherungsschutz - zumindest, wie in Abschnitt 2.5.5 gezeigt wird, bezüglich ideeller Werteverluste aus ökonomischer Rationalität nicht nachgefragt wird.

Ferner ist aus den bisherigen Ausführungen deutlich geworden, daß Kommunikationsvorgänge von multiplen Risiken bedroht werden, deren Schadenpotentiale nicht unmittelbar in monetären Einheiten gemessen werden können. Um eine theoretische ökonomische Analyse überhaupt durchführen zu können, wird die Vielzahl der Risiken, die einen Kommunikationsvorgang bedrohen, auf eine Größe, die individuelle Schadenhöhe L, reduziert. Sie wird nicht in Geldeinheiten quantitativ ausgedrückt, sondern lediglich als eine Funktion der bisher verwendeten Netzparameter aufgefaßt. Weiterhin soll der qualitative Unterschied zwischen einem po-

---

407 Hierunter fallen vor allem die Privacy (=Privatheit)-Aspekte in der Telekommunikation. Vgl. dazu u. a. Katz (1991), Noam (1991) und mit besonderem Bezug auf das ISDN Kubicek (1991). Eine kritische Einstellung gegen die Gewährung von Privacy aus ökonomischen Gründen hat Posner (1981), weil sich dadurch die asymmetrische Information zwischen den Wirtschaftssubjekten erhöht.

408 Vgl. Pommerehne (1987).

409 Privatnutzer wurden in den USA nach ihrer Zahlungsbereitschaft für die Sicherstellung von Privacy gefragt, wobei die meisten eine Zahlungsbereitschaft von unter einem Dollar pro Monat signalisierten. Vgl. dazu Katz (1991), S. 58.

410 Ein theoretisch möglicher Zugang zur Abschätzung der Wertschätzung der Sicherheitseigenschaften von Kommunikationsdiensten bietet sich durch die Untersuchung der Nachfrage nach Verschlüsselungssystemen für analoge oder digitale Telekommunikationsnetze. Jedoch ist diese auch aufgrund des hohen Preises noch so gering, daß eine Schätzung der Nachfrage mittels statistischer Regressionsverfahren noch nicht durchgeführt worden ist.

tentiellen Vermögensschaden L und dem Risiko, die immaterielle Komponente IM, z. B. in Form von Beeinträchtigungen der Privatsphäre, zu verlieren, hinsichtlich des effizienten Ausmaßes an Informationssicherheitsmaßnahmen herausgearbeitet werden.

Während die vorangegangenen Ausführungen der Charakterisierung der individuellen Schadenhöhe L und der immateriellen Komponete IM gewidmet waren, muß auch noch die Bestimmung der individuellen Schadeneintrittswahrscheinlichkeit p problematisiert werden. Eine Möglichkeit, Schadenswahrscheinlichkeiten zu bestimmen, besteht darin, Vergangenheitswerte auszuwerten und daraus durchschnittliche Eintrittswahrscheinlichkeiten abzuleiten. Praktisch scheitert dies i. d. R. daran, daß kein ausreichendes statistisches Material zur Verfügung steht.[411] Methodisch ist daran zu kritisieren, daß eine Extrapolation von Vergangenheitswerten in die Zukunft gerade durch die Dynamik der technischen Möglichkeiten im Bereich der Informations- und Kommunikationstechniken ungerechtfertigt erscheint. Außerdem existiert gerade hinsichtlich der Anzahl der Schadensfälle im Bereich der Informationssicherheit durch die unvollständige Aufdeckung ein hoher Unsicherheitsfaktor.[412]

Um das skizzierte Bewertungsproblem zu bewältigen, werden in der Praxis im Rahmen von Risikoanalysen Bewertungen der Schadensausmaße und Abschätzungen der Bedrohungsintensität durchgeführt, um daraus ein effizientes Niveau an Sicherheitsvorkehrungen abzuleiten.[413] Jedoch können sowohl für die Schadenhöhe als auch für die Schadenswahrscheinlichkeit meistens nur sehr vage Aussagen gemacht werden, so daß die ergriffenen Maßnahmen zusätzlich durch ihren diskretionären Charakter nicht den theoretischen Marginalbedingungen genügen.

Der in Teil eins der Arbeit verwendete ökonomische Zugang zu Sicherheitsvorkehrungen verlangt eine Abstraktionsebene, die von Szenarien mit multiplen Risiken absieht, auf der die Schadensgrößen L bzw. IM sowohl alle Schadensarten umfas-

---

[411] Deshalb beschränkt sich das Bundesamt für Sicherheit in der Informationstechnik (1992), S. 227, in ihren Empfehlungen für die Risikoanalyse lediglich auf eine fünfstufige Skala, die von „sehr selten“ bis „sehr häufig“ reicht.

[412] Ein Indikator für die hohe Unsicherheit mag die geringe Aufklärungsquote von 42,1% im Jahre 1993 hinsichtlich Straftaten in der Computerkriminalität sein. Vgl. dazu das Bundeskriminalamt (1994), S. 226. Im Abschnitt 2.6.2 über asymmetrische Informationsverteilung wird noch einmal auf die Bewertungsproblematik bzgl. p und L eingegangen.

[413] Eine kurze anschauliche Darstellung gibt Brandt (1993). Vgl. zur Risikoanalyse für LAN's (=Local Area Networks) Schlette (1992) oder allgemein in der Informationsverarbeitung Stelzer (1993) Kap. 6 und 7.

sen als auch in einen funktionalen Zusammenhang zu den Netzeigenschaften Größe n* und Leistungsfähigkeit I* gebracht werden können.[414] Dadurch reduziert sich auch die Vielzahl der Schadeneintrittswahrscheinlichkeiten auf eine einzige Schadenswahrscheinlichkeit p. Damit sind die Rahmenbedingungen für eine Analyse im bekannten Erwartungsnutzenmodell erfüllt. Bevor darauf und auf die funktionalen Zusammenhänge zwischen n* und I* und p, L bzw. IM eingegangen wird, bedarf es zunächst der Charakterisierung der Informationssicherheitsmechanismen und der Aufstellung einer Gesamtkostenfunktion in Abhängigkeit von den jeweiligen Eigenschaften der Kommunkationsysteme.

2.5.3 Die Kosten der Informationssicherheit in Kommunikationssystemen in Abhängigkeit von Größe und Leistungsfähigkeit

Nach der Charakterisierung der Bedrohungen in Kommunikationsnetzen werden zunächst die Sicherheitssysteme vorgestellt, die einen Schutz gegen die verschiedenen Gefährdungsarten der Informationssicherheit bieten können. Daran anschließend wird versucht, einen generellen Zusammenhang zwischen den Netzeigenschaften n* und I* und den bei der Installation von Sicherheitsmaßnahmen anfallenden Kosten herzustellen und damit eine allgemeine Kostenfunktion zu erhalten.[415] Hier muß angemerkt werden, daß es sich ebenso wie bei der übrigen Telekommunikationstechnik bei den Sicherheitssystemen um technische Standards handelt, die bei allen Teilnehmerstationen bzw. Leitungswegen identisch sein müssen, um ihre vollständige Wirksamkeit entfalten zu können. Damit haben also auch die Informationssicherheitsmechanismen in Kommunikationssystemen Clubguteigenschaften.[416]

Es wird sich hier auf die Sicherungsmechanismen beschränkt, die in Kommunikationssystemen zur Gewährleistung der Informationssicherheitseigenschaften Verfüg-

---

[414] Die Risiken können auch nach ihren Ursachen spezifiziert werden. Vgl. dazu die quantitative Aufsplittung in Näther (1991), S. 81.

[415] Konkrete Spezifizierungen von Kostenfunktionen sind heute noch nicht möglich, weil darüber keine geeigneten Daten vorliegen. Vgl. dazu Katz (1991), S. 65. Moser (1995), S. 7, führt einen Kostenvergleich zwischen Datensicherungssystemen durch, die jedoch nur für isolierte informationsverarbeitende Unternehmen geeignet sind.

[416] Von privaten teilnehmerspezifischen Informationssicherheitsmaßnahmen, wie z. B. dem Telesec der Deutschen Telekom AG, wird abgesehen.

barkeit, Integrität, Vertraulichkeit und Authentizität der Kommunikationsinhalte beitragen können.[417]

Die Verfügbarkeit von Informationen kann durch zufällige oder beabsichtigte Störungen in den Leitungen, durch Softwareprobleme in den Netzknoten und durch Nutzungsüberlastungen beeinträchtigt werden. Dagegen kann präventiv vorgegangen werden, indem ausreichende und voneinander unabhängige Übertragungskapazitäten zur Verfügung gestellt werden, eine effiziente Netzüberwachung frühzeitig Störungen und Engpässe erkennt und Redundanzen in der Netzarchitektur integriert werden.[418] Hinsichtlich der Netzteilnehmerzahl n^* muß von einem positiven Zusammenhang zwischen n^* und den Gesamtkosten für diese Sicherheitsmaßnahmen ausgegangen werden, wobei sich am Problem der Kapazitätsüberlastung deutlich machen läßt, daß hier stochastische Größenersparnisse verwirklicht werden können.[419] In größeren Netzen müssen nach dem Gesetz der großen Zahlen und der daraus folgenden besseren Kalkulierbarkeit von potentiellen Netzüberlastungen bezüglich n^* nur unterproportional Reservekapazitäten bereitgestellt werden, um einen Zusammenbruch zu verhindern. Deshalb sinken für den einzelnen Netzteilnehmer die Grenzkosten der Netzüberwachung und der Bereitstellung von Redundanzen. Dagegen wird der Integrationsgrad I^* einen positiven Einfluß auf die Grenzkosten haben, weil sowohl überproportional mehr Ersatzkapazitäten zur Überbrückung von Überlastungen bereitgestellt werden müssen als auch multilaterale Kommunikationsvorgänge im Gegensatz zu bilateralen übermäßig Redundanzen benötigen, damit auch im Schadensfall Ersatzleitungen zur Verfügung stehen.

Integrität von Kommunikationsinhalten bedeutet Schutz vor absichtlichen oder vor durch technische Defekte bedingten Veränderungen während der Übertragung. Technische Übermittlungsfehler können durch ein gleichzeitiges Senden einer Prüfsumme, welche nur bei korrekter Übermittlung mit der geforderten übereinstimmt, aufgedeckt werden. Diese Maßnahme ist jedoch gegenüber bewußten Manipulationen unwirksam, so daß zusätzliche Vorkehrungen getroffen werden müs-

---

[417] Vgl. zu Gefahren und Gegenmaßnahmen Gauthey & Haefelfinger (1991), S. 67-69. Auf eine Einordnung der Sicherungsmechanismen in das OSI-Modell wird verzichtet. Vgl. dazu Pfitzmann (1990), S. 108-114, und Schützig (1992) und zu Sicherungsmechanismen in öffentlichen Funknetzen, die auch Datenschutz i. e. S. sicherstellen können, Pfitzmann (1993).

[418] Das Prinzip der Redundanz besteht darin, immer zwei vollkommen verschiedene Übermittlungswege zur Verfügung zu haben, damit man bei Ausfall des einen den anderen benutzen kann. Vgl. dazu Zehle (1993), S. 16f.

[419] Vgl. dazu Fritsch, Wein & Ewers (1993), S. 125, und S. 167.

sen, die den später dargestellten Methoden zur Sicherung der Authentizität entsprechen.

Um die Vertraulichkeit der Kommunikationsinhalte gegenüber Abhörversuchen zu sichern, bietet sich die Verschlüsselung von Nachrichten an. Der Absender macht mittels eines Schlüssels durch einen Verschlüsselungsalgorithmus die Originalnachricht für uneingeweihte Dritte unlesbar, so daß nur der Empfänger den Inhalt nach der Entschlüsselung verstehen kann. Man differenziert die Verfahren nach symmetrischer und asymmetrischer Verschlüsselung.[420] Während beim symmetrischen Verschlüsseln, welches jeder Kommunikationsverbindung einen Schlüssel zuordnet[421], die Anzahl der benötigten Schlüssel quadratisch mit der Netzteilnehmerzahl ansteigt, verlangt das asymmetrische Verschlüsseln, das jedem Teilnehmer einen öffentlichen und einen privaten Schlüssel zuordnet, lediglich doppelt soviel Schlüssel wie Teilnehmer.[422] Wendet man also das kostengünstige asymmetrische Verschlüsselungsverfahren an und unterstellt man zusätzlich einen Fixkostenblock, der durch die Schlüsselverwaltung, d. h. Schlüsselerzeugung, -speicherung, -austausch, -archivierung und -löschung, anfällt, dann erfährt der einzelne Teilnehmer bei der Zunahme der Netzteilnehmer n* sinkende Grenzkosten. Dagegen sind in Netzen mit einem höheren Integrationsgrad I* die Grenzkosten der Chiffrierung höher, weil der Verschlüsselungsaufwand für umfangreichere Kommunikationsinhalte ansteigt und vor allem die komplexeren Kommunikationsstrukturen eine aufwendigere Schlüsselgenerierung und -verwaltung verursachen.

Schließlich gibt es eine Reihe von Kommunikationsvorgängen, bei denen sichergestellt werden muß, daß die Kommunikationspartner das Senden bzw. Empfangen von Kommunikationsinhalten nicht abstreiten können. In sonstigen vertraglichen Beziehungen sorgt dafür eine handschriftliche Unterschrift. In Kommunikationsnetzen benötigt man dazu eine elektronische Unterschrift.[423] Die geforderte Authentizität kann wiederum durch die asymmetrische Verschlüsselung erreicht wer-

---

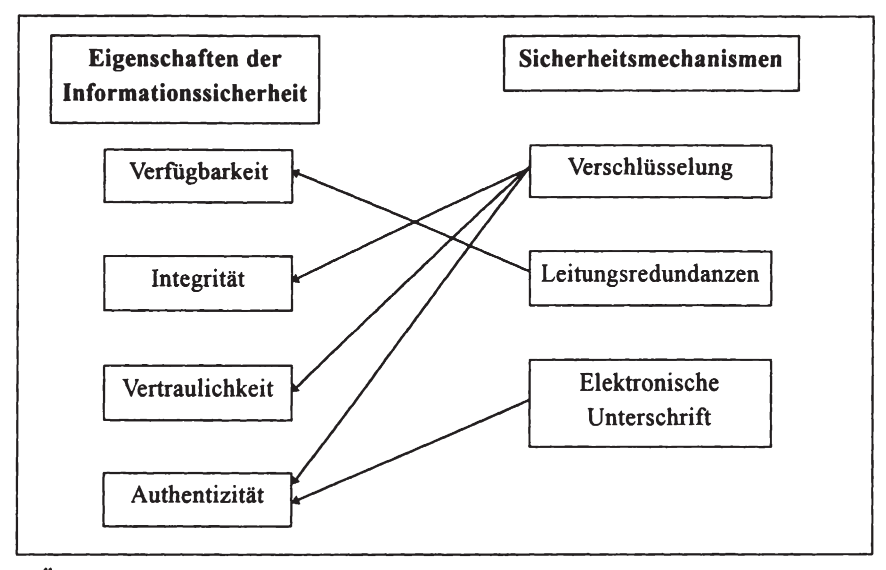
420 Vgl. genauer dazu Kündig (1989), S. 74-76.

421 Es werden genauer $[n^2-n]/2$ Schlüssel benötigt.

422 Die öffentlichen Schlüssel, mit denen die Sender verschlüsseln, stehen in einer Art öffentlichem Telefonbuch, während die privaten Schlüssel zum Entschlüsseln von den einzelnen Teilnehmern vertraulich aufbewahrt werden müssen, damit die Vertraulichkeit gewährleistet bleibt. Obwohl keine Schlüssel mehr ausgetauscht werden, muß eine vertrauenswürdige Stelle eingerichtet werden, die die Gültigkeit der öffentlichen Schlüssel der einzelnen Teilnehmer bestätigt. Eine anschauliche Darstellung asymmetrischer Verschlüsselungsverfahren findet sich in Beutelspacher (1987), Kap. 4. Vgl. zu dem Verschlüsselungsverfahren PEM im Internet Horster & Protz (1994).

423 Vgl. dazu auch die Kommission der Europäischen Gemeinschaften (1992), S. 27.

den, weil sich die Teilnehmer durch die Kenntnis des entsprechenden Schlüssel identifizieren können.[424]



Übersicht 7: Eigenschaften der Informationssicherheit und die entsprechenden Sicherheitsmechanismen

In Übersicht 7 werden die dargestellten Sicherheitsmechanismen mit den vier Eigenschaften der Informationssicherheit bei Kommunikationsvorgängen in Beziehung gestellt. Es existieren zwar noch weitere Sicherungssysteme zur Gewährleistung der Informationssicherheit[425], jedoch hat die Kostenanalyse der Maßnahmen zur Sicherstellung der verschiedenen Schutzbedürfnisse in Abhängigkeit von den Netzparametern n* und I* funktionale Zusammenhänge ergeben, die für eine theoretische Effizienzbetrachtung genügen.

Es hat sich gezeigt, daß die Gesamtkostenfunktion der einzelnen Sicherheitssysteme für das ganze Netz positiv abhängig von der Teilnehmerzahl n* ist. Jedoch nehmen durch den bei allen Mechanismen vorhandenen Fixkostenblock für den einzelnen Kommunikationsteilnehmer die Durchschnittskosten mit zunehmender

---

424 Vgl. zu den technischen Methoden der Authentifikationsprüfung im Funknetz C, in öffentlichen Kartentelefonen und in der Mobilkommunikation nach dem GSM (= Global System for Mobile Communication) Wolfenstetter (1993), S. 739ff.

425 Vgl. dazu u. a. Fumy & Riess (1993), S. 120.

Nutzerzahl ab, weil n*, wie oben gezeigt, generell nicht in der Nähe der sich durch stark ansteigende variable Kosten zusätzlicher Teilnehmer auszeichnenden Kapazitätsgrenze liegt.

Des weiteren ist die Gesamtkostenfunktion wiederum positiv abhängig vom Integrationsgrad I*. Dabei ist aber von steigenden Grenzkosten auszugehen, so daß die Sicherheitsmaßnahmen auch den einzelnen Kommunikationsteilnehmern in höher integrierten Netzen verstärkt Kosten verursachen.

Schließlich gilt es noch zu bestimmen, ob die Sicherheitsmaßnahmen nun vornehmlich auf die Reduktion der Schadeneintrittswahrscheinlichkeiten oder der Schadenhöhen ausgerichtet sind. Betrachtet man die Verschlüsselung der Kommunikationsinhalte als elementarste und universellste Sicherheitsvorkehrung[426], dann handelt es sich eindeutig um eine Maßnahme, die die Schadeneintrittswahrscheinlichkeit reduziert. Denn ein ausgereiftes Verschlüsselungs- oder Kryptoverfahren kann nur mit hohem Aufwand „geknackt“ werden, so daß die Wahrscheinlichkeit der Entschlüsselung der Kommunikationsinhalte durch Unbefugte sehr gering wird. Ist der Code aber gelöst bzw. bekannt, dann hat das Chiffrierverfahren keinen Nutzen mehr aus der Eindämmung des Schadensausmaßes.[427] Eine ähnliche Wirkung hat die Bereitstellung von Ersatzleitungen. Dadurch wird wiederum lediglich die Ausfallwahrscheinlichkeit gesenkt, falls es dennoch zu einem Zusammenbruch kommt, wird durch Redundanzen das Schadensausmaß nicht reduziert. Die Sicherheitsmechanismen in Kommunikationsnetzen haben folglich eher den Charakter von Self-protection- und weniger von Self-insurance-Maßnahmen. Deshalb wird im folgenden Abschnitt das optimale Ausmaß an Informationssicherheitsvorkehrungen unter der Annahme bestimmt, daß die eingesetzten Sicherheitssysteme ausschließlich die Schadeneintrittswahrscheinlichkeit p zu reduzieren vermögen.

Wenn man die Ergebnisse der Kostenanalyse zusammenfaßt, kann man folgende Gesamtkostenfunktion der Informationssicherheitsmaßnahmen r, welche überwie-

---

[426] Vgl. dazu auch die Kommission der Europäischen Gemeinschaften (1992), S. 24ff.

[427] Ein regelmäßiger Wechsel des Schlüssels kann jedoch auch für eine Begrenzung des Schadensausmaßes sorgen. Davon wird jedoch abstrahiert. Vgl. Heuser (1995), S. 2.

gend zur Senkung der Schadeneintrittswahrscheinlichkeiten dienen, ableiten:

$$(34)\ TC_r(n^*,I^*) = F_r(I^*) + f_r(n^*,I^*)$$
$$\text{mit } F_r(I^*)>0,\ \partial F_r/\partial I^*>0,\ \partial^2 F_r/\partial I^{*2}>0,\ \partial f_r/\partial n^*>0,\ \partial^2 f_r/\partial n^{*2}>0,$$
$$\partial f_r/\partial I^*>0,\ \partial^2 f_r/\partial I^{*2}>0 \text{ und } \partial^2 f_r/\partial n^*\partial I^*>0.$$ [428]

Unterstellt man wiederum, daß jeder einzelne Nutzer unabhängig von seiner Nutzungsintensität für die Kosten der Sicherheitsmechanismen aufkommen muß, dann ergibt sich eine Belastung in Höhe der Durchschnittskosten $AC_r = \frac{1}{n^*} \cdot (F_r(I^*) + f_r(n^*, I^*))$, wobei die Kosten für den einzelnen durch die Aufteilung des Fixkostenblocks mit zunehmender Netzgröße abnehmen ($\partial AC_r/\partial n^*<0$) und zunehmendem Integrationsgrad ansteigen ($\partial AC_r/\partial I^*>0$).

Neben dem Einfluß der exogenen Parameter n* und I* muß noch eine Charakterisierung des Gesamtkostenverlaufs in Abhängigkeit von den ergriffenen Sicherheitsmaßnahmen erfolgen. Es werden vereinfachend hinsichtlich der Sicherheitsvorkehrungen konstante Grenzkosten in Höhe von AC_r vorausgesetzt, so daß für den einzelnen Netzteilnehmer Gesamtkosten in Höhe des Produktes aus dem Ausmaß an Sicherheitsmaßnahmen[429] r und Grenz- bzw. Durchschnittskostenkosten AC_r anfallen. Aufgrund der nachlassenden Wirkung der Maßnahmen hinsichtlich der Senkung der Schadeneintrittswahrscheinlichkeit steigt der Aufwand für jede weitere prozentuale Reduktion der Schadenswahrscheinlichkeit an, so daß auf diesem indirekten Wege ein progressiver Grenzkostenverlauf zu verzeichnen ist.

---

[428] Es handelt sich um die gleiche Kostenstruktur, die in Abschnitt 2.4 in den Kostenfunktionen der Gleichungen (28) bzw. (31) unterstellt wurde. Erst bei Erreichen der Kapazitätsgrenzen werden die variablen Kosten eines zusätzlichen Nutzers die Fixkostendegression aufwiegen. Geht man jedoch davon aus, daß sich die einzelnen Netze nur bis zur optimalen Nutzerzahl n* ausdehnen, dann ist dieser Bereich progressiver Kostenverläufe nicht relevant.

[429] Darunter kann man z. B. die Häufigkeit der Verschlüsselungen der Kommunikationsinhalte oder die Anzahl der vorhandenen Ersatzleitungen verstehen.

2.5.4 Das effiziente Ausmaß an Informationssicherheit in Kommunikationsnetzen und -diensten in Abhängigkeit von Größe und Leistungsfähigkeit

2.5.4.1 Das Ausgangsszenario

Bevor nachfolgendend theoretische Effizienzbedingungen abgeleitet werden, wird kurz auf die aktuelle Situation der Installation von Informationssicherheitsmechanismen eingegangen. In offenen Kommunikationssystemen wie dem Telefonnetz sind zur Zeit keine der vorgestellten Informationssicherungsmechanismen netzweit implementiert[430], weil dies in den alten analogen Leitungen nicht möglich und in den neuen digitalen im Moment noch nach Angaben von Mitarbeitern des damit befaßten Produktzentrums Telesec der Deutschen Telekom AG auch nicht genau zu kalkulierende Kosten verursachen würde. Ausnahmen bilden die auf dem GSM-Standard basierenden Mobilfunksysteme, die eine Verschlüsselung der Funkstrekken vornehmen.[431] Deshalb haben Großkonzerne wie die Daimler-Benz AG, Stuttgart, ein eigenes Informationssicherheitskonzept entwickelt, das die Datenübertragung auf internen und den öffentlich zugänglichen Kommunikationsystemen umfaßt.[432]

Die Realität außer acht lassend, wird in diesem Abschnitt ausgehend von einem Kommunikationsnetz, welches durch die Parameter Teilnehmerzahl n^* und den Integrationsgrad I^* definiert ist, das effiziente Ausmaß an Informationssicherheitsmaßnahmen in offenen Kommunikationssystemen bestimmt. Dabei kommen durch die öffentliche Gutseigenschaft bzw. durch den gemeinsamen Standard der Informationssicherheitsmechanismen alle Teilnehmer in gleichem Maße in den Genuß der daraus resultierenden Informationssicherheit.[433]

---

430 Die Abteilung Telesec der Deutschen Telekom AG bietet jedoch einzelnen Teilnehmern bzw. Teilnehmergruppen verschiedene Informationssicherheitssysteme an, die jedoch noch mehrere Tausend DM kosten.

431 Vgl. zu den informationstechnischen Sicherheitsmechanismen in der Mobilkommunikation Peters (1995).

432 Vgl. Staudinger (1995).

433 Um die Komplexität der individuellen Entscheidung zu reduzieren, wird von Rückwirkungen des Sicherheitsniveaus auf n^* und I^* abgesehen. Ein alternatives Vorgehen ist, zusätzlich zu diesen Parametern auch das gewährte Informationssicherheitsniveau heranzuziehen. Es wird außerdem von privaten bzw. lokalen Maßnahmen wie z. B Zugangskontrollsystemen abgesehen, weil sie die durchschnittliche Informationssicherheit im Netz nicht beeinflussen können. Vgl. zur Differenzierung von lokalem und globalem bzw. netzbezogenen Sicherheitsmanagement Näther (1991), S. 85.

Es wird sich hier auf die Vorgehensweise von Kapitel 1.2 bezogen, wo nach dem Prinzip der Erwartungsnutzenmaximierung die volkswirtschaftlich effiziente Allokation von Sicherheitsgütern bzw. Produktsicherheit abgeleitet wird. Wiederum eine Zwei-Punkt-Wahrscheinlichkeitsverteilung unterstellend, falle mit der Wahrscheinlichkeit p bei einem Kommunikationsvorgang in einem durch n* und I* definierten Netz dem betrachteten Individuum ein Schaden in Höhe von L bzw. eine Nutzeneinbuße IM an, während mit der Wahrscheinlichkeit (1-p) die Informationssicherheit während des Kommunikationsvorganges nicht beeinträchtigt wird.

Bevor der Erwartungsnutzen bestimmt werden kann, muß noch herausgearbeitet werden, welchen Einfluß die Netzeigenschaften n* und I* auf Schadenswahrscheinlichkeit p und Schadenhöhe L bzw. IM haben. Grundsätzlich beeinflussen n* und I* sowohl p als auch L bzw. IM, jedoch werden folgende Vereinfachungen vorgenommen, wobei von Einflüssen des Aktivitätsniveaus, d. h. der Anzahl der Kommunikationsvorgänge, abgesehen wird. Die Schadenhöhe L und die Nutzenkomponente IM hängen wesentlich vom Integrationsgrad I* ab, weil mit I* auch die monetäre und ideelle Wertschätzung der Kommunikationsinhalte zunehmen wird. Denn leistungsfähigere Netze oder Dienste bieten zusätzlich zu denen des einfachen Netzes weitere Übertragungsmöglichkeiten, so daß dadurch auch ein potentiell höherer Schaden generiert wird[434], während die Anzahl der Netzteilnehmer n* vernachlässigt werden kann[435], so daß gilt:

$$(35) \quad L = L(I^*) \text{ mit } \partial L/\partial I^* > 0 \text{ und } \partial^2 L/\partial I^{*2} \leq 0 \text{ bzw.}$$

$$(35') \quad IM = IM(I^*) \text{ mit } \partial IM/\partial I^* > 0 \text{ und } \partial^2 IM/\partial I^{*2} \leq 0.$$

Im Gegensatz zur Schadenhöhe beeinflußt n* die Schadenswahrscheinlichkeit p maßgeblich, weil mit n* sowohl die Leitungswege und -knoten als auch die geheimzuhaltenden Schlüssel und damit die potentiellen Fehlerquellen bzw. Angriffsflächen zunehmen. Außerdem haben Informationen die Eigenschaft der Nichtrivalität im Konsum und können damit mehreren Individuen gleichzeitig Nutzen stiften. Deshalb ist es aber auch möglich, daß bei einem Schadensfall in Kommuni-

---

434 Der maximale potentielle kommerzielle und ideelle Verlust durch das Mithören eines „normalen" Telefongesprächs ist geringer als derjenige durch das Verändern oder Kopieren ganzer Dateien, weil der Umfang und damit auch der Wert der transportierten Inhalte zunehmen. Vgl. dazu auch Kubicek (1991a), S. 54.

435 Aufgrund der nahezu kostenlosen Vervielfältigung von Informationen bzw. von Kommunikationsinhalten ist n* für die Schadenhöhe nahezu bedeutungslos. Bzgl. des Datenschutzes i. e. S. sind aber mit der Zunahme der Kommunikationsmöglichkeiten aussagekräftigere Bewegungsprofile möglich.

kationsnetzen gleichzeitig Sender und Empfänger negativ tangiert werden. Dadurch wird auch ein positiver Zusammenhang zwischen I* und p unmittelbar einsichtig. Zwar muß mit steigendem Integrationsgrad die durchschnittliche Schadenswahrscheinlichkeit nicht unbedingt ansteigen, jedoch wird durch die damit verbundene höhere Leistungsfähigkeit, welche u. a. Kommunikationsvorgänge zwischen mehr als zwei Teilnehmern ermöglicht, der positive Einfluß der Gesamtteilnehmerzahl n* auf die individuelle Schadenswahrscheinlichkeit p erhöht. Eine Studie des National Research Council, Board on Telecommunications and Computer Application aus dem Jahre 1989 nennt vier Gründe, warum in höher integrierten Netzen die Wahrscheinlichkeit eines Systemausfalls ansteigt. Erstens wirken sich durch die Konzentration von Funktionen Ausfälle einzelner Netzkomponeten auf weite Netzbereiche aus. Zweitens zieht die zunehmende Komplexität der benötigten Software erhöhte Sofware-Fehlerraten nach sich.[436] Drittens muß verstärkt mit Software-Angriffen gerechnet werden, und schließlich nimmt die relative Häufigkeit von Ausfällen durch Feuer, Erdbeben und Sabotageakten zu. Im weiteren wird deshalb von folgenden Beziehungen ausgegangen:

$$(36) \quad p = p(n^*, I^*)$$
$$\text{mit } \partial p/\partial n^*>0,\ \partial^2 p/\partial n^{*2}\leq 0,\ \partial p/\partial I^*>0,\ \partial^2 p/\partial I^{*2}\leq 0 \text{ und } \partial^2 p/\partial n^*\partial I^*>0.$$

I* kann gewissermaßen als Korrelationskoeffizient aufgefaßt werden. Bei $I^*=0$ sind die Schadensfälle stochastisch unabhängig, so daß die individuelle Schadenswahrscheinlichkeit p unabhängig von der Netzteilnehmerzahl n* ist. Dagegen kann bei positiven Werten von I* ein Schaden gleichzeitig bei mehreren Teilnehmern eintreten, so daß mit größerer Teilnehmerzahl auch die Schadenswahrscheinlichkeit für den einzelnen stärker zunimmt. Im Extremum $I^*=1$ sind die Kommunikationsteilnehmer so stark miteinander verbunden, daß ein Schadensfall unmittelbar alle Netzteilnehmer trifft.[437]

Schließlich muß noch auf den Einfluß von n* und I* auf Ausgangsausstattung bzw. -vermögen W eingegangen werden. Das Kommunikationssystem mit n* und I* bringt den betrachteten Individuen im Vergleich zu anderen Netzen den größten Nutzen bzw. die höchste Konsumentenrente ein. Dieser durch einen Kommunikati-

---

436 Vgl. dazu auch Lütge (1995), S. 19.

437 Eine negative Korrelation der Schadensfälle wird in einer statischen Betrachtung ausgeschlossen, weil es keine plausible Begründung dafür gibt, warum nach Eintritt eines Schadenfalls bei einem Netzteilnehmer das Schadenrisiko der anderen sinkt. Bei der Diskussion um die Versicherbarkeit in Abschnitt 2.5.5.2 wird die Bedeutung von I* als Schadenskorrelationsindikator nochmals aufgegriffen.

onsanschluß erreichte Nutzenzuwachs kann prinzipiell als Anstieg des Ausgangsvermögens W interpretiert werden. Jedoch wird davon ausgegangen, daß die in monetären Einheiten gemessene Konsumentenrente eines Netzanschlusses auch für Individuen mit anderen Präferenzen ungefähr dieselbe ist, so daß von einem Einfluß von n* und I* auf W abgesehen werden kann.[438]

Ohne zunächst irgendwelche Sicherheitsmaßnahmen zu berücksichtigen, berechnet sich deshalb der individuelle Erwartungsnutzen aus einem Anschluß an ein Kommunikationsnetz mit n* und I* bei einem reinem potentiellen materiellen Schaden L entsprechend der Konstellation von Abbildung 14 wie folgt:

$$(37)\quad \begin{aligned} E\left[U^T(w_1)\right] &= p(n^*,I^*)\left[U_{12}(W-L(I^*))+IM_{12}\right] \\ &\quad +(1-p(n^*,I^*))\left[U_{11}(W)+IM_{11}(W)\right]>0. \end{aligned}$$

Bei möglichen Nutzeneinbußen durch den Verlust immaterieller Werte, z. B. wegen einer durch Telefonabhörungen verletzten Privatsphäre, bestimmt sich der Erwartungsnutzen nach (37'):

$$(37')\quad \begin{aligned} E\left[U^T(w_1)\right] &= p(n^*,I^*)\left[U_{11}(W)\right] \\ &\quad +(1-p(n^*,I^*))\left[U_{11}(W)+IM_{11}(W)\right]>0 \end{aligned}$$

Neben der Möglichkeit, keine Sicherheitsmaßnahmen zu ergreifen, bleiben dem Individuum analog zum Vorgehen in Kapitel 1.2 theoretisch drei weitere Handlungsmöglichkeiten.[439] Jedoch hat die Darstellung der verschiedenen Sicherheitsmaßnahmen in Kommunikationsnetzen gezeigt, daß es sich hierbei um Vorkehrungen handelt, die die individuelle Schadeneintrittswahrscheinlichkeit p zu reduzieren vermögen.[440]

---

[438] Es wird also KR=U(n*,I*)-P(n*,I*) als konstant und damit unabhängig von n* und I* angenommen. Genaugenommen geht das Ausgangsvermögen selbst mit positivem Vorzeichen in die Schadenhöhe ein, weil davon auszugehen ist, daß der Verlust der verschiedenen Attribute der Informationssicherheit, die eine Einkommenselastizität größer eins aufweisen, trotz abnehmendem Grenznutzen bei wohlhabenderen Personen einen höheren Schaden verursachen wird. Jedoch werden Individuen mit höherem Vermögen leistungsfähigere Kommunikationssystem wählen, so daß dieser Zusammenhang indirekt über I* in die Schadenhöhe einfließt.

[439] Vgl. dazu Übersicht 1.

[440] In der Realität erfolgt die Steigerung des Sicherheitsniveaus durch die Installation von Sicherheitssystemen in diskreten Schritten. Hier bietet sich die Annahme von stetig abnehmenden Fehlerwahrscheinlichkeiten bei zunehmenden Self-protection-Maßnahmen an. Außerdem wird in der Telema-

Der individuelle Nutzen ohne Sicherheitsmaßnahmen und bei Self-protection		
Der Verlust materieller Werte		
	potentielle Nutzenzustände	
Handlungsalternativen	S=1 (Normalfall)	S=2 (Schadensfall)
a=1 (keine Sicherheitsmaßnahmen)	$U_{11}(W)+IM_{11}(W)$	$U_{12}(W-L(I^*))$ $+IM_{12}(W-L(I^*))$
Wahrscheinlichkeiten	$1-p(n^*, I^*)$	$p(n^*, I^*)$
a=2 (Self-protection)	$U_{21}(W-rAC_r(n^*, I^*)$ $+IM_1(W-rAC_r(n^*, I^*))$	$U_{22}(W-L-rAC_r(n^*,I^*)$ $+IM_{22}(W-L-rAC_r(n^*,I^*))$
Wahrscheinlichkeiten	$1-p(r, n^*, I^*)$	$p(r, n^*, I^*)$
Der Verlust reiner immaterieller Werte		
	potentielle Nutzenzustände	
Handlungsalternativen	S=1 (Normalfall)	S=2 (Schadensfall)
a=1 (keine Sicherheitsmaßnahmen)	$U_{11}(W)+IM_{11}(W)$	$U_{11}(W)$
Wahrscheinlichkeiten	$1-p(n^*,I^*)$	$p(n^*,I^*)$
a=2 (Self-protection)	$U_{21}(W-rAC_r(n^*, I^*))$ $+IM_{21}(W-rAC_r(n^*,I^*))$	$U_{21}(W-rAC_r(n^*, I^*))$
Wahrscheinlichkeiten	$1-p(r,n^*,I^*)$	$p(r,n^*,I^*)$

Übersicht 8: Individueller Nutzen ohne Schutzmaßnahmen und mit Self-protection

Deshalb werden die anderen theoretisch möglichen Präventionsstrategien wie Self-insurance nicht mehr betrachtet. Die Untersuchung konzentriert sich dagegen auf

---

tik Sicherheit oft in Wahrscheinlichkeiten bzw. Zuverlässigkeiten gemessen. Vgl. dazu u. a. Pfitzmann (1990), S. 244ff.

die qualitativen Unterschiede zwischen den ökonomisch effizienten Sicherheitsniveaus bei drohenden Vermögensverlusten und immateriellen Schäden. Außerdem wird im darauf folgenden Abschnitt die Versicherungsmöglichkeit von Kommunikationsrisiken, welche dieselben Implikationen wie Schadenbegrenzungs- bzw. Self-insurance-Maßnahmen hat, dargestellt und besonders in bezug auf die Problematik nicht ersetzbarer Werte diskutiert. In Übersicht 8 sind zunächst die potentiellen Nutzenzustände im Ausgangszustand und bei Ergreifung von Self-protection-Maßnahmen hinsichtlich der qualitativ unterschiedlichen Schadensfallkonstellationen zusammengestellt.

2.5.4.2 Das optimale Ausmaß an Self-protection zur Gewährleistung der Informationssicherheit

Nachdem die Ausgangssituation ohne Sicherheitsvorkehrungen im vorangegangenen Abschnitt definiert wurde, geht es nun darum, das optimale Ausmaß an Self-protection r* auf der Basis einer Erwartungsnutzenmaximierung für den Fall materieller und immaterieller Schäden zu bestimmen.[441]

Die Grenz- bzw. Durchschnittskosten AC_r der Informationssicherheitsmechanismen r wurden schon in Gleichung (34) in Abhängigkeit von n* und I* bestimmt. Nun muß noch ihr Einfluß auf die Schadeneintrittswahrscheinlichkeit p charakterisiert werden. Selbstverständlich wird diese durch die Installation von Sicherheitssystemen reduziert, so daß gilt: $\partial p/\partial r < 0$.[442] Jedoch nimmt ihre Grenzproduktivität mit zunehmendem r, formal ausgedrückt als $\partial^2 p/\partial r^2 > 0$, ab. Von einem negativen Einfluß von n* und I* auf die Effektivität der Maßnahmen kann abgesehen werden, weil beide schon einen positiven Einfluß auf das Niveau der ursprünglichen Schadenswahrscheinlichkeit p(n*,I*) haben.

Es gilt nun also den Erwartungsnutzen in Gleichung (38) bzw. (38′) durch die Variation von r zu maximieren:

$$(38) \quad \max_r E\left[U^T\right] = p(r,n^*,I^*)\cdot\left[U_{22}+IM_{22}\right]+(1-p(r,n^*,I^*))\cdot\left[U_{21}+IM_{21}\right]$$

$$\text{bzw. } (38') \quad \max_r E\left[U^T\right] = p(r,n^*,I^*)\cdot\left[U_{21}\right]+(1-p(r,n^*,I^*))\cdot\left[U_{21}+IM_{21}\right].$$

---

[441] Einen diskretionären Ansatz der Kosten-Nutzen-Analyse bzgl. Datensicherungsmaßnahmen gemäß §9 BDSG und seine Umsetzung in die Praxis stellt Volle (1995) vor.

[442] Vgl. dazu bzgl. allgemeiner kollektiver Sicherheitsmaßnahmen Cook & Graham (1977), S. 151ff.

Die Bedingung erster Ordnung für ein Erwartungsnutzenmaximum im Fall von Vermögensschäden lautet dann:[443]

$$
(39)\quad
\begin{aligned}
&p(r,n^*,I^*)\cdot\left[U_{22}'(-AC_r(n^*,I^*)+IM_{22}'(-AC_r(n^*,I^*))\right]\\
&+p'(r)\left[U_{22}+IM_{22}\right]\\
&+(1-p(r,n^*,I^*))\cdot\left[U_{21}'(-AC_r(n^*,I^*)+IM_{21}'(-AC_r(n^*,I^*))\right]\\
&-p'(r)\cdot\left[U_{21}+IM_{21}\right]\overset{!}{=}0.
\end{aligned}
$$

Nach einer Umformung kommt man auf die Effizienzbedingung (39′):

$$
(39')\quad
\begin{aligned}
MB_r &= \frac{-p'(r^*)\cdot\left[U_{21}+IM_{21}-U_{22}-IM_{22})\right]}{p(r^*,n^*,I^*)\cdot\left[U_{22}'+IM_{22}'\right]+(1-p(r^*,n^*,I^*))\cdot\left[U_{21}'+IM_{21}'\right]}\\
&\overset{!}{=}AC_r(n^*,I^*).
\end{aligned}
$$

Im Erwartungsnutzenoptimum ist der individuelle Grenznutzen MB_r in Form der marginalen Senkung des Nutzenverlustes ($\Delta U^T=U_{21}+IM_{21}-U_{22}-IM_{22}$), der mit einem von der Risikoaversion abhängigen Term gewichtet ist, gleich den Grenzkosten AC_r.[444]

Die Bedingung erster Ordnung bei potentiellem Verlust von IM leitet sich entsprechend aus der Erwartungsnutzenmaximierung von (38′) ab:[445]

$$
(40)\quad
\begin{aligned}
&p(r,n^*,I^*)\cdot\left[U_{21}'(-AC_r(n^*,I^*)\right]+p'(r)\left[U_{21}\right]\\
&+(1-p(r,n^*,I^*))\cdot\left[U_{21}'(-AC_r(n^*,I^*)+IM_{21}'(-AC_r(n^*,I^*))\right]\\
&-p'(r)\cdot\left[U_{21}+IM_{21}\right]\overset{!}{=}0.
\end{aligned}
$$

$$
\text{bzw. (40')}\quad MB_r' = \frac{-p'(r^*)\cdot IM_{21}}{U_{21}'+(1-p(r^*,n^*,I^*))IM_{21}'}\overset{!}{=}AC_r(n^*,I^*).
$$

---

443 Die partiellen Ableitungen der Nutzenkomponenten werden jeweils mit U′und IM′ bezeichnet.

444 Die hinreichende Bedingung zweiter Ordnung für ein Maximum lautet: $\left[AC_r\right]^2\left[(1-p(r^*,n^*,I^*)\left[U_{21}''+IM_{21}''\right]+p(r^*,n^*,I^*)\left[U_{22}''+IM_{22}''\right]\right]+p''(r^*)\left[U_{22}+IM_{22}-U_{21}-IM_{21})\right]$ $+2\cdot AC_r\cdot p'(r^*)\left[U_{21}'+IM_{21}'-U_{22}'-IM_{22}')\right]<0.$
Damit diese Bedingung erfüllt ist, muß der letzte Summand dem Betrag nach kleiner sein als die Summe der ersten beiden Summanden. Es gibt zwar Spezialfälle, in denen dies nicht der Fall ist, es wird jedoch im weiteren von der Erfüllung der Bedingung zweiter Ordnung ausgegangen.

445 Dionne (1982), S. 410ff, kommt im Rahmen der Analyse von Moral Hazard bei „state dependent utility functions“ zu einem ähnlichen Ergebnis.

Nach der Effizienzbedingung aus Gleichung (40′) wird das Individuum solange Maßnahmen zur Senkung der Schadeneintrittswahrscheinlichkeit tätigen bis der Grenznutzen, die mit dem Nutzen des ideellen Wertes ($\Delta U^{T\prime}=IM_{21}$) gewichtete marginale Senkung der Schadeneintrittswahrscheinlichkeit, gleich den Grenzkosten AC_r entspricht.[446]

Bevor der Einfluß der beiden Netzparameter Größe n* und Leistungsfähigkeit I* auf r* näher untersucht wird, lohnt es sich, einen Vergleich der Effizienzbedingungen von Self-protection bei Vermögensschäden L und durch den Verlust von IM bedingten, immateriellen Nutzeneinbußen anzustellen. Eine geeignete Vergleichsbasis kann dadurch hergestellt werden, daß zum einen die Grenzproduktivität von r in beiden Fällen identisch ist und daß zum anderen der Nutzenverlust hinsichtlich des Gesamtnutzens U^T gleich ist ($\Delta U^T=U_{21}+IM_{21}-U_{22}-IM_{22}=\Delta U^{T\prime}=IM_{21}$). Die weitere Annahme gleicher Grenzkosten AC_r erlaubt schließlich die Gleichsetzung der linken Seiten der Effizienzbedingungen (39′) und (40′), was zu folgender Gleichheitsbedingung führt:

$$(41)\quad \begin{aligned} & p(r^*,n^*,I^*)\cdot\left[U_{22}'+IM_{22}'\right]+(1-p(r^*,n^*,I^*))\cdot\left[U_{21}'+IM_{21}'\right] \\ & =U_{21}'+(1-p(r^*,n^*,I^*))IM_{21}' \end{aligned}.$$

Nach einer Umformung ergibt sich schließlich folgende einfache Beziehung:

$$(41')\quad U_{22}'+IM_{22}'=U_{21}'.$$

Da U_{22}' durch die Konkavität der Nutzenfunktion bezüglich des Vermögens immer größer ist als U_{21}', muß IM_{22}' einen negativen Wert annehmen, damit Gleichung (41′) erfüllt ist.[447] Dies bedeutet jedoch, daß die Nutzenkomponente IM mit steigendem Vermögen abnimmt und es sich damit um ein inferiores Gut handeln muß.[448] Da aber gerade der Verlust der Vertraulichkeit von Kommunikationsbeziehungen für Personen mit höherem Vermögen im Vergleich zu weniger wohlhaben-

---

446 Die Bedingung zweiter Ordnung für ein Maximum lautet wie folgt:

$$\left[AC_r\right]^2\left[(1-p_i(r^*,n^*,I^*)\left[U_{21}''+IM_{21}''\right]+p(r^*,n^*,I^*)\left[U_{21}''\right]\right]+p''(r^*)\left[IM_{21}\right]+2\cdot AC_r\cdot p'(r^*)\left[IM_{21}'\right]<0.$$

Sie ist erfüllt, wenn der mittlere Term dem Betrage nach kleiner ist als die beiden übrigen. Um Ecklösungen auszuschließen, wird dies auch unterstellt.

447 Es kann generell argumentiert werden, daß es sich bei IM′>0 bei dem ideellen Wert um ein Komplement und bei IM′<0 um ein Substitut zum Vermögen w handelt. Vgl. dazu Hirshleifer & Riley (1992), S. 62.

448 Für Cook & Graham (1977), S. 147 FN 9, und Shioshansi (1982), S. 315, ist ein unersetzbares Gut dann ein normales Gut, wenn der horizontale Abstand zwischen den Nutzenfunktionen bei zunehmendem Vermögen zunimmt, welches auch den Regelfall darstellt und zum hier angewandten Ansatz kein Widerspruch darstellt..

den Individuen abgesehen von möglichen Vermögensschäden eine absolut höhere ideelle Nutzeneinbuße darstellt, wie es auch in Abbildung 14 unterstellt wird, ist Voraussetzung (41´) i. d. R. nicht erfüllt, und es gilt statt dessen für $IM_{22}' \geq 0$:

$$(42) \quad U_{22}' + IM_{22}' > U_{21}'.$$

Blickt man dann auf die ursprüngliche Vergleichssituation der Gleichungen (39´) und (40´) zurück, bedeutet dies, daß der Grenznutzen von Self-protection MB_r' im Fall von ideellen Wertverlusten höher ist als der Grenznutzen MB_r bei identischer Nutzeneinbuße durch Vermögensverluste, so daß das optimale Ausmaß an Aufwendungen für Self-protection r* deshalb bei Verlustrisiken hinsichtlich ideeller Werte umfangreicher ist als bei reinen Vermögensschäden. Abbildung 15 stellt einen unmittelbaren Vergleich der Grenznutzen zusätzlicher Schadensprävention-maßnahmen r in den jeweiligen Fällen bei identischen Grenzkosten AC_r dar.

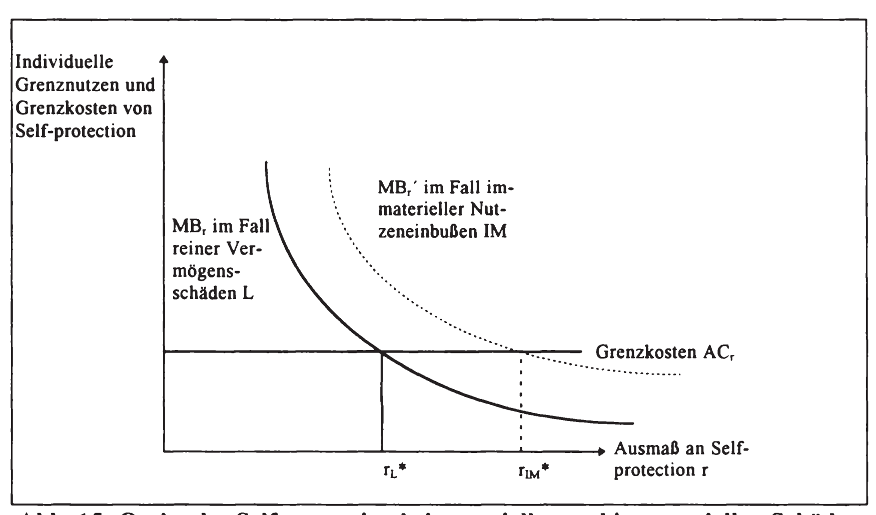


Abb. 15: Optimales Self-protection bei materiellen und immateriellen Schäden

Bei einem als identisch unterstellten Grenzkostenverlauf der Self-protection-Maßnahmen ist es im Vergleich zu Vermögensrisiken effizient, ein umfangreicheres Ausmaß an Sicherheitsmaßnahmen bei Verlustrisiken mit immateriellen Charakter zu ergreifen ($r_{IM}^* > r_L^*$), weil der Grenznutzen der Sicherheitsmaßnahmen für letz-

teren Fall höher ist.[449] In der Realität sollten deshalb aus nutzentheoretischer Sicht bei der Implementierung von Informationssicherheitsmechanismen in Kommunikationssystemen, die stark von Privatpersonen genutzt werden bzw. deren Mißbrauch potentiell zu Verletzungen der Privatsphäre führt, im Vergleich zu ähnlichen, aber kommerziell genutzten Netzen nicht gespart, sondern eher verstärkt Ressourcen für Informationssicherheit eingesetzt werden.

Um nun die Beziehung zwischen der Größe n* bzw. der Leistungsfähigkeit I* der Netze zum effizienten Ausmaß an Informationssicherheitsmaßnahmen bestimmen zu können, muß strenggenommen das totale Differential von Gleichung (39′) bzw. (40′) gebildet werden. Aus Anschaulichkeitsgründen wird im folgenden jedoch von einem risikoneutralen Individuum ausgegangen, so daß zum einen die Unterscheidung in Vermögensschäden L und Beeinträchtigungen immaterieller Werte hinfällig wird[450] und sich das Effizienzkriterium (39′) zu folgender Bedingung (43) vereinfacht:

$$(43) \qquad AC_r(n^*, I^*) = -p'(r^*) \cdot L(I^*).$$

Bildet man nun das totale Differential von (43), dann kommt man zu Gleichung (44):

$$(44) \qquad \frac{\partial AC_r}{\partial n^*} \cdot dn^* + \frac{\partial AC_r}{\partial I^*} \cdot dI^* = -p'(r^*) \cdot \frac{\partial L}{\partial I^*} \cdot dI^* - L(I^*) \cdot \frac{\partial p'}{\partial r^*} \cdot dr^*.$$

Betrachtet man zunächst die Beziehung zwischen der Leistungsfähigkeit I* und dem optimalen Niveau an Self-protection r*, geht man von einem konstanten n* aus, setzt deshalb dn*=0 und kommt durch Umformen auf:

$$(45) \qquad \frac{dr^*}{dI^*} = -\frac{\dfrac{\partial AC_r}{\partial I^*} + p' \cdot \dfrac{\partial L}{\partial I^*}}{L \cdot \dfrac{\partial p'}{\partial r^*}}.$$

Da der Ausdruck im Nenner nach $\partial^2 p/\partial r^2 > 0$ ein positives Vorzeichen hat, ist das nicht eindeutige Vorzeichen des Zählers entscheidend. Gilt $\frac{\partial AC_r}{\partial I^*} > -p' \cdot \frac{\partial L}{\partial I^*}$, dann nimmt

---

[449] Man kann dieses Ergebnis auch damit begründen, daß sich das Individuum bei potentiellen Vermögensverlusten einer höheren Grenzkostenkurve als bei immateriellen Risiken gegenübersieht. Denn ausgehend von den Bedingungen (39′) und (40′) gilt bei Risikoaversion immer:

$$AC_r[U_{21}' + (1 - p(r^*, n^*, I^*))IM_{21}'] < AC_r[(1 - p(r^*, n^*, I^*))(U_{12}' + IM_{21}') + p(r^*, n^*, I^*)(U_{22}' + IM_{22}')].$$

[450] Dabei wird auch noch die implizite Annahme getroffen, daß die immaterielle Komponente IM nicht vom Vermögen abhängt (IM′=0).

das optimale Ausmaß an Sicherheitsvorkehrungen in höher integrierten Netzen ab, weil der Grenzkostenanstieg den Grenznutzenanstieg durch verhinderte Schadensfälle überkompensiert. Umgekehrt verhält es sich dagegen, wenn $\frac{\partial AC_r}{\partial I^*} < -p' \cdot \frac{\partial L}{\partial I^*}$ gilt. Denn dann ist der Grenznutzen zusätzlicher Sicherheitsmaßnahmen größer als die anfallenden Grenzkosten, so daß es in leistungsstärkeren Netzen ökonomisch effizient ist, verstärkt Informationssicherheitsmaßnahmen zu ergreifen.

Eindeutig verhält es sich hinsichtlich der Beziehung von der Netzgröße n* zu r*. Geht man entsprechend von einem gegebenen Integrationsgrad aus, setzt man analog dI*=0 und kommt zu folgender Relation:

$$(46) \quad \frac{dr^*}{dn^*} = -\frac{\frac{\partial AC_r}{\partial n^*}}{L \cdot \frac{\partial p'}{\partial r^*}}.$$

In diesem Quotienten ist sowohl das Vorzeichen des Zählers als auch des Nenners eindeutig bestimmbar. Denn für den Nenner gilt dasselbe wie in Gleichung (45). Der Zähler ist dagegen eindeutig negativ, so daß in größeren Netzen durch die mit der steigenden Teilnehmerzahl fallenden Grenzkosten auch pro Teilnehmer verstärkt Informationssicherheitsmaßnahmen ergriffen werden sollten.

Diese Ergebnisse gelten eigentlich nur für den Spezialfall risikoneutraler Netzteilnehmer. Da aber kein eindeutiger Zusammenhang zwischen dem Grad der Risikoaversion und dem Ausmaß an optimalen Sicherheitsvorkehrungen besteht[451], wird im weiteren die Untersuchung auf diesen Ergebnissen aufgebaut. Deshalb hängt das optimale Ausmaß an Informationssicherheitsmaßnahmen bezogen auf den einzelnen Teilnehmer wie folgt von Größe n* und Leistungsfähigkeit I* der Kommunikationssysteme ab:

$$(47) \quad r^* = r^*(\underset{+}{n^*}, \underset{?}{I^*}).$$

Ausgehend von dem funktionellen Zusammenhang in Gleichung (47) können im folgendem die optimalen Niveaus an Sicherheitsmaßnahmen in den Kommunikationsnetzen in Abhängigkeit von n* und I* graphisch bestimmt werden. In Abbildung 16 wird unmittelbar deutlich, daß in Netzen mit höheren Teilnehmerzahlen

---

451 Vgl. dazu u. a. Nell (1993), S. 74.

das optimale Ausmaß an Informationssicherheit höher ist als in kleineren Netzen, weil trotz identischer Grenznutzen MB_r[452] die Grenzkosten AC_r in teilnehmerstärkeren Kommunikationssystemen geringer sind.

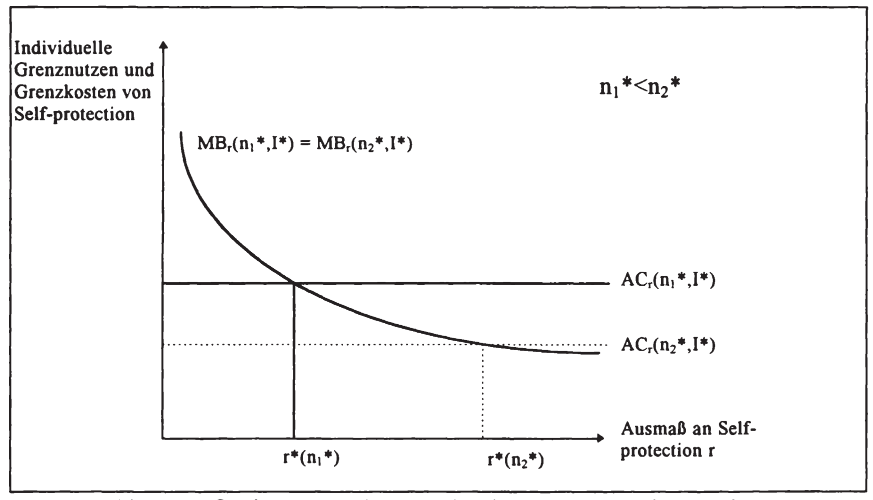


Abb. 16: Optimales Self-protection in unterschiedlich großen Kommunikationssystemen

Dagegen bleibt, wie Abbildung 17 auf der folgenden Seite zeigt, unklar, ob in einem Netz mit einem höheren Integrationsgrad mehr oder weniger Maßnahmen zur Reduktion der Schadeneintrittswahrscheinlichkeit ergriffen werden sollten. Es wird die Situation abgebildet, in welcher der Anstieg der Grenzkosten verhältnismäßig geringer ausfällt als die Zunahme der Grenznutzen in Form der Reduktion des Erwartungsschadens.

Davon ausgehend, daß es sich bei den Systemen zur Sicherung von Verfügbarkeit, Vertraulichkeit, Integrität und Verbindlichkeit der Kommunikationsinhalte um Maßnahmen handelt, die zur Senkung der Schadeneintrittswahrscheinlichkeit beitragen können, wurde das optimale Niveau an Informationssicherheitsmaßnahmen r^* in Abhängigkeit der Netzcharakteristika Teilnehmerzahl n^* und Integrationsgrad I^* bestimmt. Aufgrund des Rückgangs der individuellen Grenzkosten mit zunehmender Teilnehmerzahl, sollten in teilnehmerstärkeren Netzen in jedem Fall sowohl ein absolut als auch relativ höheres Ausmaß für Informationssicherheit be-

[452] Nach Effizienzbedingung (43) wird nicht die Grenznutzen-, sondern nur die Grenzkostenseite von der Netzgröße n^* beeinflußt.

trieben werden. Dies bedeutet, daß durch die steigenden Nutzerzahlen zum einen der Gesamtaufwand für Sicherheitsmaßnahmen zunehmen sollte und zum anderen durch die noch stärkere Splittung der Gesamtkosten die Grenzkosten für den einzelnen absinken, so daß auch auf den einzelnen Teilnehmer bezogen die Sicherheitsvorkehrungen ansteigen sollten.

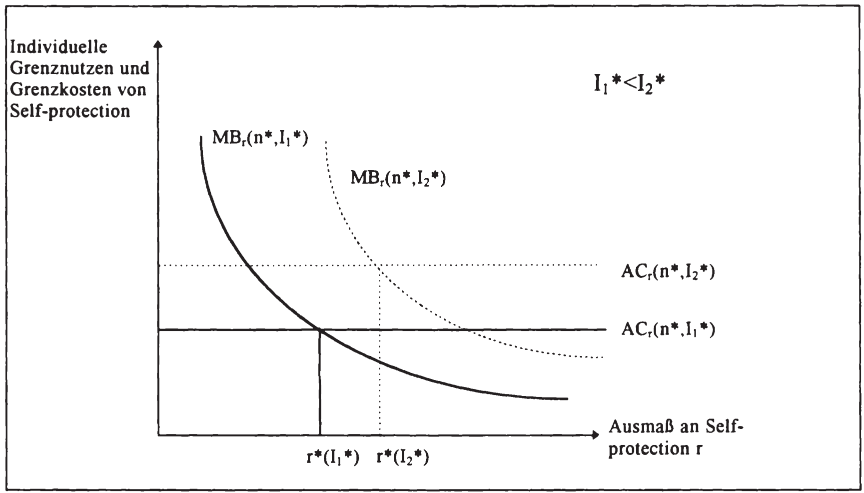


Abb. 17: Optimales Self-protection in unterschiedlich leistungsfähigen Kommunikationssystemen

Dagegen verlangt ein gehobener Integrationsgrad bzw. ein leistungsfähigeres Kommunikationssystem nur dann einen umfangreicheren Einsatz von Sicherheitssystemen, wenn der Anstieg der Grenzkosten geringer ausfällt als die Ausweitung des individuellen Schadenpotentials. Da aber die Sicherheitsmechanismen in allen Netzen grundsätzlich nach dem gleichen Prinzip funktionieren, werden die Grenzkosten nicht stark ansteigen bzw. aufgrund der verbesserten Technologie in Zukunft sogar absinken, während die durch zusätzliche Kommunikationsmöglichkeiten entstehenden Schadenpotentiale auf jeden Fall zunehmen. Deshalb sollten aus Effizienzgesichtspunkten in den leistungsfähigeren Kommunikationssystemen der Zukunft verstärkt Informationssicherheitsmaßnahmen installiert werden.

Schließlich zeigt der nutzentheoretische Vergleich von reinen Vermögensschäden und dem Verlust immaterieller Nutzenkomponenten, daß Kommunikationsvorgänge, welche bei potentiellen Verletzungen der Informationssicherheit vor allem Persönlichkeits-

rechte bedrohen, besonders durch Informationssicherungsmaßnahmen geschützt werden müssen.

2.5.5 Zur Versicherung von Informationssicherheitsrisiken in Kommunikationsnetzen und -diensten

2.5.5.1 Vorbemerkungen

Neben den technischen Maßnahmen zur Prävention der Informationssicherheitsrisiken in Kommunikationsnetzen und -diensten bietet sich grundsätzlich die Versicherungslösung als weiteres Instrument des Risikomanagements an. In einem ersten Schritt wird überprüft, unter welchen Bedingungen diese Risiken offener Kommunikationssysteme von einem privaten Versicherer versicherbar sind. Anschließend wird die Versicherungsnachfrage unter der Annahme einer fairen Prämiengestaltung bei Vermögens- und immateriellen Schäden theoretisch abgeleitet. Im dritten Abschnitt wird eine Übersicht über das aktuelle Versicherungsangebot bezüglich Informationsrisiken in der Bundesrepublik Deutschland gegeben, bevor mögliche ökonomische Gründe für eine staatliche Einflußnahme auf das private Versicherungsangebot diskutiert werden.

2.5.5.2 Die notwendigen Bedingungen der privaten Versicherbarkeit von Informationssicherheitsrisiken

Bevor die eigentliche Nachfrage nach Versicherung von durch die Nutzung von Kommunikationsnetzen verursachten Risiken bestimmt werden kann, muß zunächst untersucht werden, ob die allgemeinen Bedingungen für ein privates Versicherungsangebot hinsichtlich so gearteter Schadenpotentiale generell erfüllt sind.

In der versicherungsökonomischen Literatur werden gemeinhin fünf Bedingungen unterschieden, die erfüllt sein müssen, damit ein privater Versicherer einen Versicherungsschutz anbietet.[453] Bei der Untersuchung wird sich wiederum auf die beiden allgemeinen Eigenschaften von Kommunikationssystemen Größe und Leistungsfähigkeit bezogen.

---

[453] Vgl. zu den folgenden Ausführungen u. a. Rejda (1992) S. 24-26. Eine ausführliche Darstellung verschiedener Standpunkte zur Versicherbarkeit von Risiken liefert Lucius (1979), S. 200-228.

Als Grundbedingung muß gelten, daß eine hinreichend große Zahl von Individuen potentiell durch gleichartige Risiken bedroht ist, damit der Versicherer aufgrund des Gesetzes der großen Zahlen eine durchschnittliche Schadenswahrscheinlichkeit und -höhe berechnen kann. Dies ist bei den Kommunikationsteilnehmern der verschiedenen Kommunikationsnetze und -dienste der Fall, weil die Teilnehmerzahl n^* mindestens eine hinreichend große kritische Masse n_k überschreitet und grundsätzlich alle Teilnehmer von denselben Risiken bedroht werden.

Zum zweiten muß der Schadensfall zufällig und unbeabsichtigt sein, weil damit das Marktversagen verursachende Moral Hazard[454] ausgeschlossen wird und der Versicherer die durchschnittlichen Schadenswahrscheinlichkeiten aufgrund des stochastischen Gesetzes der großen Zahlen berechnen kann. Obwohl Schadensfälle in Kommunikationsnetzen im wesentlichen entweder durch technische Defekte oder durch beabsichtigte Angriffe von Dritten verursacht werden, kann nicht ausgeschlossen werden, daß im Einzelfall Versicherungsnehmer selbst einen Schadensfall absichtlich herbeiführen, um in den Genuß der Versicherungsleistung zu kommen. Jedoch können die Versicherer durch bestimmte Versicherungsvertragskomponenten, wie den Selbstbehalt des Versicherungsnehmers, ihre Versicherungsleistungen so beschränken, daß die Versicherungsnehmer i. d. R. keinen Anreiz haben, Schadensfälle absichtlich herbeizuführen.

Es muß zum dritten möglich sein, den Eintritt des Schadenfalls und die Schadenhöhe mit Sicherheit zu bestimmen. In den meisten Fällen können technische Defekte in Kommunikationssystemen und die daraus folgenden Schäden bestimmt werden. Bei einem Teil der Verletzungen der Informationssicherheit in Kommunikationsnetzen und -diensten kann der Eintritt des Schadenfalls nicht objektiv nachgewiesen werden. So sind Verletzungen der Verfügbarkeit und der Integrität von Kommunikationsinhalten und die unrechtmäßige Authentizität von Kommunikationspartnern im allgemeinen - wenn auch nicht immer unmittelbar - nachweisbar. Dagegen gibt es für die Nichteinhaltung der Vertraulichkeit nur dann eine Beweismöglichkeit, wenn ein objektiv belegbarer Folgeschaden ausgelöst wird, der mit der Vertraulichkeitsverletzung in unmittelbarem Zusammenhang steht. Dies ist ein Grund dafür, warum Schäden hervorgerufen durch die nicht gewährte Vertraulichkeit der Kommunikationsinhalte nur bedingt von einem privaten Anbieter zu versichern sind. Ein zweiter Grund liegt darin, wie in Abschnitt 2.5.2 ausgeführt und in Abbildung 14 dargestellt, daß so geartete Schäden, besonders wenn sie einen Ver-

---

454 Vgl. dazu Abschnitt 1.3.4.

lust der immateriellen Nutzenkomponente IM darstellen, von verschiedenen Individuen gemeinhin unterschiedlich intensiv empfunden werden. Der Versicherer hat dadurch im Gegensatz zu materiellen Vermögenseinbußen keinen eindeutigen Maßstab für seine Kompensationsleistungen und wird deshalb ex ante mit dem Versicherten eine bestimmte monetäre Entschädigung festlegen müssen. Hierbei ist jedoch darauf zu achten, daß die Verbesserung der Vermögenssituation für das Individuum nicht zu einem Nutzenanstieg im Schadensfall führt, weil damit Anreize zur Selbstverursachung des Schadens geschaffen werden. Dagegen können materielle Schäden, die durch die Zerstörung oder Veränderung von durch Kommunikationssysteme übermittelten Informationen hervorgerufen werden, durch den Aufwand zur Wiederherstellung der ursprünglichen Kommunikationsinhalte und durch die Kosten der Stornierung von Kommunikationsvorgängen, die nicht authentifizierte Kommunikationsteilnehmer erteilten, relativ einfach bestimmt werden. Des weiteren ist die Gefahr von Moral Hazard nicht gegeben, wenn lediglich die ursprüngliche Vermögensposition wiederhergestellt wird.

Zum vierten dürfen die Schäden nicht katastrophale Ausmaße in dem Sinne annehmen, daß im Schadensfall ein großer Teil der Versicherten bzw. der Kommunikationsteilnehmer gleichzeitig einen Schaden erleidet. Denn dann stellen die individuellen Schadensfälle keine unabhängigen Ereignisse mehr dar. Diese Unabhängigkeit ermöglicht aber der Versichertengemeinschaft bzw. dem Versicherungsanbieter, jedem Versicherten vollständigen Schutz vor den finanziellen Folgen im Schadensfall zu bieten. Ist sie nicht gegeben, droht dem Versicherer im Schadensfall bei fairen Prämien die Illiquidität, und er ist dazu gezwungen, die Prämien mit der Folge eines Versicherungsnachfragerückganges zu erhöhen.

Bezogen auf die Informationssicherheitsrisiken kann deshalb gefolgert werden, daß in leistungsfähigen Kommunikationssystemen mit einem hohen Integrationsgrad I*, der gemäß der Definition in Abschnitt 2.5.4.1 das Ausmaß der Korrelation der individuellen Schadensfälle signalisiert, die Unabhängigkeit der Einzelschäden und dadurch die Versicherbarkeit durch einen privaten Versicherer nicht mehr gegeben ist. Konkret bedeutet dies, daß Verletzungen der Informationssicherheit im Rahmen von multilateralen Kommunikationsvorgängen gleichzeitig bei mehreren Teilnehmern einen Schaden anrichten, so daß im Kontext eines einzigen Schadenfalls im Kommunikationssystem an die Versicherung mehrere Entschädigungsansprüche gestellt werden. Hier wird der Versicherer zusätzlich damit konfrontiert, daß er die Gesamtkompensation auf die Betroffenen aufzuteilen hat bzw. daß die simultane Kompensation mehrerer Geschädigter kollektives Moral Hazard hervorrufen kann.

Hinsichtlich des negativen Zusammenhangs zwischen einem steigenden Integrationsgrad I* der Kommunikationssysteme und der damit schwieriger werdenden Versicherbarkeit der Risiken durch einen privaten Versicherer kann jedoch nur eine qualitative Aussage getroffen werden. Denn im Fall von Bagatellschäden bedroht eine starke Abhängigkeit der Individualschäden die Existenz des Versicherers nicht unbedingt, während bei sehr hohen Schadenssummen selbst eine geringe Korrelation die Rücklagen der Versicherungsgesellschaft unzumutbar stark belasten. Als Lösung bietet es sich für den Versicherer bei katastrophalen Schäden in komplexen Kommunikationssystemen an, daß ein Rückversicherer für Schadenskompensationsforderungen, die ein gewisses maximales Gesamtschadensausmaß überschreiten, aufkommt.

Fünftens muß der Versicherer dazu in der Lage sein, sowohl durchschnittliche Schadenswahrscheinlichkeiten als auch Schadenhöhen mit einer gewissen Genauigkeit zu berechnen, damit eine verlustdeckende Prämienfestsetzung möglich ist. Treten Schadensereignisse unregelmäßig und auch in unterschiedlicher Intensität auf, dann sind solche Berechnungen einer hohen Fehlerwahrscheinlichkeit unterworfen. Prinzipiell können diese Größen auf Basis von Vergangenheitswerten auch für die Risiken von Informationssicherheitsverletzungen in Kommunikationssystemen bestimmt werden. Jedoch treten dabei zwei Probleme auf. Zum einen existiert nur begrenzt aussagefähiges statistisches Material, weil technische Defekte nicht systematisch registriert werden und die niedrige Aufklärungsrate bei Delikten der Computerkriminalität[455], welche auch die kriminellen Aktionen in Kommunikationsnetzen umfaßt, von einer hohen Dunkelziffer im Hinblick auf die eigentliche Zahl an Straftaten zeugt. Zum anderen weiten sich mit den technischen Möglichkeiten der Kommunikationsnetze und -dienste auch die Schadenpotentiale aus, so daß eine Extrapolation von Vergangenheitswerten in die Zukunft nur bedingt möglich ist.

Schließlich muß der Versicherte bereit sein, die geforderte Versicherungsprämie zu bezahlen. Diese muß deshalb wesentlich unter dem Nennwert der Versicherungspolice liegen. Damit diese Bedingung erfüllt ist, sollte die Schadenswahrscheinlichkeit i. d. R. unter 40% liegen. Denn ansonsten liegen die Gesamtkosten des Versicherungsvertrages einschließlich Verwaltungskosten und damit auch die Prämien so weit über der vereinbarten Versicherungsleistung, daß in diesen Fällen für potentielle Versicherungsnachfrager kein Anreiz besteht, einen Versicherungsver-

[455] Vgl. Fußnote 412.

trag abzuschließen.[456] Damit die einzelnen Individuen einen Versicherungsschutz erlangen können, müssen sie also Informationssicherheitsmaßnahmen ergreifen, welche die Schadenseintrittswahrscheinlichkeiten auf ein versicherbares Niveau drücken.

Abgesehen von den Gefahren, die vor allem beim Verlust der Vertraulichkeit im Rahmen der Übermittlung von Kommunikationsinhalten eine bedeutende immaterielle Nutzenkomponente beinhalten, und der hohen Korrelation von Schadensereignissen in leistungsfähigen und komplexen Kommunikationsnetzen und -diensten sind die Bedingungen der Versicherbarkeit durch einen privaten Versicherer oder durch eine von den Kommunikationsteilnehmern selbst organisierte Versichertengemeinschaft hinsichtlich der übrigen Risiken für die Informationssicherheit in offenen Kommunikationssystemen erfüllt. Damit kann in einem nächsten Schritt jeweils die individuelle Nachfrage nach Versicherungsschutz gegen so verursachte Vermögensschäden und immateriellen Nutzeneinbußen theoretisch abgeleitet und einem Vergleich unterzogen werden.

2.5.5.3 Die Versicherungsnachfrage hinsichtlich durch Verletzungen der Informationssicherheit hervorgerufene Vermögensschäden

Das betrachtete Individuum bzw. ein repräsentative Kommunikationsteilnehmer sei mit den in der folgenden Übersicht 9 dargestellten Risikoszenarien konfrontiert. Nun bestehe zusätzlich zur Ergreifung von Informationssicherheitsmaßnahmen die Möglichkeit, sich gegen potentielle Schäden, die durch die Verletzung der Informationssicherheit in Kommunikationssystemen entstehen können, zu versichern. In diesem Abschnitt werden zunächst Vermögenseinbußen untersucht, die durch eine Verletzung der Verfügbarkeit, der Integrität und der Vertraulichkeit der Kommunikationsinhalte und durch falsche Authentifizierungen von Kommunikationsteilnehmern entstehen können.

---

[456] Dies Versicherungsprämie P darf deshalb die Summe aus Erwartungsschaden ES und individueller Risikoprämie R nicht überschreiten.

Der individuelle Nutzen mit und ohne Versicherungsschutz		
bei Verlust reiner materieller Werte		
	potentielle Nutzenniveaus	
Handlungsalternativen	S=1 (Normalfall)	S=2 (Schadensfall)
a=1 (keine Versicherung)	$U_{11}(W)+IM_{11}(W)$	$U_{12}[W-L(I^*)]$ $+IM_{12}[W-L(I^*)]$
Wahrscheinlichkeiten	$1-p(n^*, I^*)$	$p(n^*, I^*)$
a=3 (Versicherung)	$U_{31}[W-p(n^*,I^*)dL(I^*)]$ $+IM_{31}[W-p(n^*,I^*)dL(I^*)]$	$U_{32}[W-(1-d(1-p(n^*,I^*))$ $L(I^*)]$ $+IM_{32}[W-(1-d(1-$ $p(n^*,I^*))L(I^*)]$
Wahrscheinlichkeiten	$1-p(n^*, I^*)$	$p(n^*, I^*)$
bei Verlust reiner immaterieller Werte		
	potentielle Nutzenzustände	
Handlungsalternativen	S=1 (Normalfall)	S=2 (Schadensfall)
a=1 (keine Versicherung)	$U_{11}(W)+IM_{11}(W)$	$U_{11}(W)$
Wahrscheinlichkeiten	$1-p(n^*,I^*)$	$p(n^*,I^*)$
a=3 (Versicherung)	$U_{31}[W-p(n^*, I^*)dK]$ $+IM_{31}[W-p(n^*,I^*)dK]$	$U_{32}[W-(1-d(1-p(n^*,I^*))K]$
Wahrscheinlichkeiten	$1-p(n^*,I^*)$	$p(n^*,I^*)$

Übersicht 9: Individueller Nutzen ohne und mit Versicherungsschutz

Analog zur Vorgehensweise in Abschnitt 1.2.3.4 kann das Individuum seinen Erwartungsnutzen durch die Wahl des Deckungsgrades d, definiert als Quotient aus der geleisteten Kompensation K des Versicherers im Schadensfall und dem Vermögensverlust L, maximieren. Darüberhinaus wird unterstellt, daß es dem Individuum möglich ist, den Versicherungsschutz zu aktuarisch fairen Prämien zu erwerben, so

daß die Prämie gleich dem mit dem Deckungsgrad multiplizierten Erwartungsschaden ES=pL ist. Es gilt deshalb den Erwartungsnutzen aus Gleichung (48) mittels Variation des Entscheidungsparameters d zu maximieren:

$$(48) \quad \max_{d} E\left[U^T\right] = p(n^*, I^*) \cdot \left[U_{32} + IM_{32}\right] + (1 - p(n^*, I^*) \cdot \left[U_{31} + IM_{32}\right],$$

mit $U_{31}=U_{31}[W\text{-}p(n^*,I^*)dL(I^*)]$, $IM_{31}=IM_{31}[W\text{-}pdL(I^*)]$, $U_{32}=U_{32}[W\text{-}(1\text{-}d(1\text{-}p(n^*,I^*))L(I^*)]$ und $IM_{32}=IM_{32}[W\text{-}(1\text{-}d(1\text{-}p(n^*,I^*)L(I^*)]$. Nach der Bedingung erster Ordnung für ein Erwartungsnutzenmaximum müssen sich die Grenznutzen in beiden Situationen ausgleichen, so daß gelten muß:[457]

$$(49) \qquad U_{31}' + IM_{31}' = U_{32}' + IM_{32}'.$$

Vernachlässigt man die Grenznutzenterme bezüglich des ideellen Wertes IM bzw. setzt man sie gleich, dann muß der Grenznutzen des Vermögens im Schaden- und im Nichtschadensfall identisch sein, was gleichzeitig einen Deckungsgrad d=1 und damit dem Standardergebnis des vollständigen Versicherungsschutzes entspricht.[458]

Hinsichtlich der Versicherungsnachfrage bei Vermögensrisiken, verursacht durch die verschiedenen Gefährdungen der Informationssicherheit in Kommunikationssystemen, ergibt sich bei fairen Prämiensätzen logischerweise das traditionelle Ergebnis der Vollversicherung.

2.5.5.4 Die Versicherungsnachfrage bei Nutzeneinbußen durch den Verlust eines ideellen Wertes

Im Gegensatz zum vorangegangenen Abschnitt soll nun von einer Nutzeneinbuße bedingt durch den Verlust des ideellen Wertes IM ausgegangen werden, der mit der Nutzung von Kommunikationssystemen verbundenen Verletzung der Privatsphäre

---

[457] Die Bedingung 2. Ordnung des Maximierungsproblems ist bei Risikoaversion der Individuen in allen Nutzenkomponenten immer erfüllt.

[458] Unterstellt man auch bzgl. IM einen mit dem Vermögen abnehmenden Grenznutzen $IM''<0$, dann bedeutet dies $IM_{32}'>IM_{31}'$ und führt unmittelbar zu $U_{31}'>U_{32}'$, welches nur durch einen Deckungsgrad $d>1$ erreicht werden kann. Im Gegensatz dazu implizieren $IM'<0$ und $IM''>0$ einen Deckungsgrad $d<1$.

in Form eines mitgehörten privaten Telefongesprächs erklärt werden kann.[459] Es handelt sich mit Bezug auf Abbildung 18 zunächst um die Konstellation (A, B′).

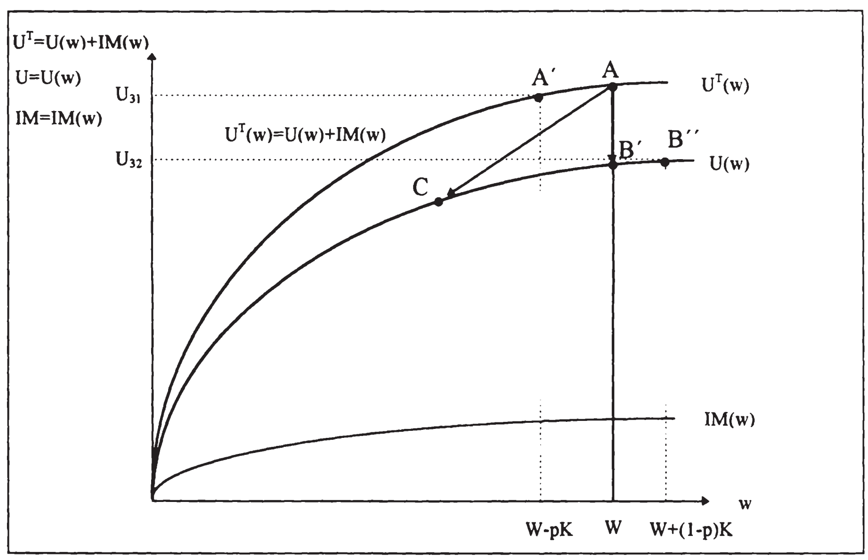


Abb. 18: Nutzenkonstellation bei Versicherung immaterieller Werte

Das Individuum habe nun die Möglichkeit, eine Versicherung abzuschließen, die ihm bei Verlust von IM zumindest eine monetäre Kompensation in Höhe von K bezahlt, während er im Gegenzug eine Prämie in Höhe der erwarteten Kompensation pK entrichtet.[460] In Bezug auf Abbildung 18 handelt es sich um die Konstellation (A′, B′′). Nun gilt es unter der Wahl von K, die folgende Erwartungsnutzenfunktion zu maximieren:

$$(50) \quad \max_K E\left[U^T\right] = p(n^*,I^*)\cdot\left[U_{32}\right] + (1-p(n^*,I^*))\cdot\left[U_{31}+IM_{31}(I^*)\right]$$

---

459 Im Gegensatz zu den theoretischen Untersuchungen von Shioshansi (1982), S. 316f, Dionne (1982) und Schlesinger (1984), S. 133f, kommt es hier nicht, wie in Abbildung 18 durch Punkt C dargestellt, zu einem gleichzeitigen Vermögensverlust.

460 Um Moral Hazard bzgl. der Schadeneintrittswahrscheinlichkeit auszuschließen, sei die Kompensation K so niedrig, daß sie das Individuum nicht indifferent zwischen Schaden- und Nichtschadensfall mache. Hinsichtlich der Schadenhöhe ist kein ex post Moral Hazard möglich, weil die Höhe der Kompensation K schon ex ante festgelegt wird.

mit $U_{31}=U_{31}[W-p(n^*,I^*)K]$, $IM_{31}(I^*)=IM_{31}[W-p(n^*,I^*)K]$ und $U_{32}=U_{32}[W+(1-p(n^*,I^*))K)]$. Die Bedingung erster Ordnung für ein Erwartungsnutzenmaximum lautet wie folgt:[461]

$$(51) \quad U_{31}'+IM_{31}'=U_{32}'.$$

Ist die Nutzenkomponente IM bzw. der Nutzen aus einer ungestörten Privatsphäre im Bereich der Kommunikationsbeziehungen, die durch die dargestellten Informationssicherungsmechanismen erreicht werden kann, unabhängig von der Vermögensposition ($IM'=0$), dann wird sich das Individuum nicht versichern. Dies bedeutet, daß sich die Nutzenfunktion U(w) von der Gesamtnutzenfunktion $U^T(w)$ nur durch eine Parallelverschiebung unterscheidet und die Grenznutzen zusätzlichen Vermögens im Schadens- und Nichtschadensfall bereits ohne Versicherung identisch sind.[462] Gilt dagegen $IM'>0$, wie es in Abbildung 18 dargestellt ist, dann muß der Grenznutzen des Vermögens im Schadensfall U_{32}' größer sein als derjenige im Nichtschadensfall U_{31}', was durch die Konkavität der Nutzenfunktion gleichbedeutend ist mit einer negativen Kompensation im Schadensfall und einer positiven Erstattung im Nichtschadensfall. Dies kommt einer Wette gleich, in der das Individuum auf den Nichtschadensfall setzt.[463] Bezieht man man den realistischen Fall, in Abbildung 18 durch die Konstellation (A, C) repräsentiert, mit ein, daß im Schadensfall neben dem Verlust der immateriellen Komponenten IM i. d. R. auch ein Vermögensschaden L eintritt, dann wird sich das Individuum gegen letzteren nicht mehr voll versichern.[464]

Nur bei $IM'<0$ wird das Individuum eine Versicherung mit einer zu zahlenden Prämie $P=pK$ abschließen, die ihm bei Verlust von IM eine Kompensation in Höhe von K bezahlt.[465] Dies bedeutet, daß Individuen sich nur dann gegen die immate-

---

461 Vgl. bzgl. der Bedingung 2. Ordnung eines Erwartungsnutzenmaximums Fußnote 457.

462 Es muß $W-pK=W+(1-p)K$ bzw. $K=0$ gelten. Vgl. dazu auch Abbildung 3 in Schlesinger (1984), S. 135, und Fall 1 der Fallunterscheidung von Dionne (1982), S. 412.

463 Entsprechend Abbildung 18 bedeutet dies, daß für den Nichtschadensfall A′ nicht links, sondern rechts von A liegt und daß im Schadensfall B′′ sich statt dessen auf eine Position links von B′ verschiebt. Vgl. auch Abbildung 2.7 in Hirshleifer & Riley (1992), S. 63.

464 Vgl. dazu Fall 2 der Fallunterscheidung von Dionne (1982), S. 412.

465 Dieses Ergebnis bestätigt die Überlegungen von Dionne (1982), widerspricht aber dem Resultat von Cook & Graham (1977), die ihre Analyse über die Versicherbarkeit von nichtersetzbaren Werten auf die horizontalen Abstände zwischen den Nutzenfunktionen im Schadens- und im Nichtschadensfall beziehen und verallgemeinert die Überlegungen von Schlesinger (1984), der seine Untersuchung der Versicherungsnachfrage bzgl. immaterieller Risiken unter der Annahme $IM'=0$ durchführt und offen läßt, unter welchen Bedingungen von $IM'\neq 0$ es zu einer Über- oder Unterversicherung kommt.

riellen Risiken der Informationssicherheit von Kommunikationssystemen versichern werden, wenn der Nutzen, den sie aus ihren immateriellen Nutzenkomponenten ziehen, mit zunehmendem Vermögen zurückgeht.[466] Dieser kausale Zusammenhang ist in der Realität jedoch nicht zu beobachten, denn gerade vermögendere Personengruppen haben auch unter Vernachlässigung von Vermögensaspekten einen höheren Nutzen aus einer geschützten Privatsphäre als Individuen mit einem geringeren Lebensstandard. Dies läßt sich u. a. daran belegen, daß Volkswirtschaften mit einem hohen Bruttosozoalprodukt pro Kopf wie die USA, die Bundesrepublik und Kanada die Vorreiterrolle bei der internationalen Normung von Informationssicherheitsbewertungskriterien von Informations- und Kommunikationstechniken übernommen haben[467], und daß die Datenschutzregelungen für Telekommunikationsdienstleistungen in Europa in den reichen Ländern, wie in Schweden und in den Niederlanden, am ausgeprägtesten sind.[468]

Wird man sich gegen immaterielle Risiken versichern, dann kann die finanzielle Kompensation K im Schadensfall u. U. so gewählt werden, daß dadurch eine Verbesserung des Nutzenniveaus relativ zum Nichtschadensfall erreicht wird und gleichzeitig bei Nichtbeobachtbarkeit durch den Versicherer Anreize zu Moral Hazard bzw. zur Reduktion von Self-protection-Maßnahmen ausgelöst werden.[469]

Faßt man die Ergebnisse der Analyse der Versicherungsnachfrage bezüglich Informationssicherheitsrisiken zusammen, können folgende Schlüsse gezogen werden. Hinsichtlich Vermögensrisiken, die durch die Verletzung der Informationssicherheit in Kommunikationsnetzen oder -diensten verursacht werden, wird analog zu sonstigen Risikopotentialen eine Vollversicherung nachgefragt. Im Gegensatz dazu wird für Risiken immaterieller Werte, wie eine geschützte Privatsphäre in Kommunikationsbeziehungen, die für die Mehrheit der Teilnehmer in einem komplementären Verhältnis ($IM'>0$) zur individuellen Vermögenssituation steht, überhaupt kein Versicherungsschutz verlangt. Bei Individuen, für die der betrachtete immaterielle Wert ein Substitut ($IM'<0$) zum Vermögen darstellt, besteht nach Abschluß einer Versicherung u. U. ein massiver Anreiz zur Selbstverursachung des Schaden-

466 Ein erwartungsnutzenmaximierendes Individuum wird infolgedessen die Konstellation (A, B′) in Abbildung 18 nicht gegen (A′, B′′) eintauschen.

467 Vgl. dazu Pfitzmann & Rannenberg (1993).

468 Vgl. dazu Garbe (1992).

469 Vgl. dazu Fall 3 der Fallunterscheidung von Dionne (1982), S. 413, und die daran anschließende Diskussion über die relative Bedeutung von Moral Hazard in „state dependent utility functions“ in ebenda S. 413ff.

falls, so daß es sich für die Versicherungsunternehmen nicht auszahlt, solch einen Versicherungsschutz bereitzustellen.[470]

2.5.5.5 Der aktuell angebotene Versicherungsschutz gegen Verletzungen der Informationssicherheit in offenen Kommunikationssystemen

In diesem Abschnitt wird das Spektrum des Versicherungsangebots in der Bundesrepublik Deutschland dahingehend untersucht, für welche der angesprochenen Informationsicherheitssrisiken in offenen Kommunikationsnetzen Versicherungsmöglichkeiten existieren und für welche kein Versicherungsschutz zu erhalten ist. Obwohl keine speziellen Versicherungen gegen die Risiken der Informationssicherheit in offenen Kommunikationssystemen existieren, bieten dennoch die Versicherungen zur Abdeckung von EDV-Risiken für manche Komponenten einen Versicherungsschutz.[471] Im folgenden werden deshalb die wichtigsten EDV-Versicherungen danach untersucht, inwieweit sie geeignet sind, die Schäden aus den angesprochenen Gefahren abzudecken.

Da im Vorfeld eine Begrenzung auf die Schäden, die durch Nichtgewährung von Verfügbarkeit, Integrität und Vertraulichkeit von Kommunikationsinhalten in Kommunikationsnetzen und durch unrechtmäßige Authentizität der Teilnehmer verursacht werden, getroffen worden ist, wird auf die häufig nachgefragte Elektronik-Versicherung als Versicherung der Kommunikationshardware, wie den Komponenten von Fernmeldeanlagen, nicht weiter eingegangen, obwohl sie auch Datenträger und Systemprogrammdaten aus Betriebssystemen umfaßt.[472]

Die Datenträgerversicherung kann als Komplement zur Elektronik-Versicherung angesehen werden, weil durch sie Daten aus Dateien und serienmäßig oder individuell hergestellten Programmen und die entsprechenden Datenträger, wie Disket-

---

[470] Hier kann eine Parallele zur Rechtsprechung gezogen werden, wo immaterielle Schäden oder sog. Nichtvermögensschäden nach § 253 BGB nicht ersetzt werden. Dies kann allokationstheoretisch als Selbstbehalt des Geschädigten interpretiert werden, der Anreize zu Moral Hazard verhindert. Vgl. dazu Adams (1989), S. 213ff, und allgemeiner zu ökonomischen Analyse immaterieller Schäden im Schadensrecht Schäfer & Ott (1986), S. 227-240.

[471] Vgl. zum folgenden besonders die aktuelle Übersicht des Deutschen Versicherungs-Schutzverbandes (1992), Engels (1991) und Heidinger & Andrich (1987), S. 139-161.

[472] In einer Studie der KES-Sicherheitsstudie 1994 hatten 72% der befragten Datenverarbeitungsbetreiber eine Elektronik-Versicherung abgeschlossen. Vgl. dazu Gartner & Konrad (1994), S. 13. 1993 standen der Beitragssumme von über 800 Mio. DM ein Schadenaufwand von 570 Mio DM gegenüber. Vgl. Schopka (1994), S. 9. Vgl. ausführlich zur Elektronik-Versicherung Meyer-Reim (1992).

ten, gegen Beschädigung und Zerstörung, die sowohl absichtlich als auch unabsichtlich oder durch externe Einflüsse an den Datenträgern verursacht werden, versichert sind. Da auch hier eine Beeinträchtigung der Hardware bzw. des Datenträgers Voraussetzung für eine Kompensation durch den Versicherer ist, wird nur näher auf eine erweiterte Datenträgerversicherung, nämlich auf die Software-Versicherung eingegangen, weil in dieser auch Schäden aus Datenveränderung ohne Hardware-Fehler und aus der Datenfernübertragung mitinbegriffen sind. Die Software-Versicherung deckt also die Schäden durch Datenverlust oder -zerstörung bei Kommunikationsvorgängen ab, die durch fehlerhafte Bedienung, den Vorsatz Dritter, Sabotage und Böswilligkeit, einschließlich Programm- und Datenmanipulation, verursacht werden können. Deshalb ist der Geltungsbereich dieser Versicherung auch nicht auf einen bestimmten Versicherungsort begrenzt. Der Versicherer leistet im Schadensfall eine Entschädigung in Höhe der notwendigen Kosten für die Wiederherstellung der Datenbestände. Da ex ante dieser Wert nur bedingt oder überhaupt nicht zu ermitteln ist, droht den Versicherten von seiten des Versicherers der Einwand der Unterversicherung, dem sie durch einen Selbstbehalt von 5% bzw. von mindestens DM 1000,- entgehen können. Außerdem beschränken die führenden Versicherungsunternehmen die Entschädigung bei Schadensfällen ohne Datenträgerbeeinträchtigungen auf 25% bzw. 50% der vereinbarten Versicherungssumme bzw. auf maximal 1 Million DM.[473] Außerdem ist dem Versicherungsnehmer vertraglich auferlegt, in einem bestimmten Zeitabstand Sicherungskopien der versicherten Datenbestände anzufertigen.

Neben der Versicherung gegen den unmittelbaren Schaden durch Datenmanipulation oder -zerstörung können auch Folgeschäden, wie der verlorengegangene Betriebsgewinn oder Mehrkosten der Betriebsfortführung, im Rahmen einer Elektronik-Betriebsunterbrechungs-Versicherung und einer Elektronik-Mehrkostenversicherung abgedeckt werden, wobei durch die zahlreichen Ausschlußklauseln lediglich Entschädigungsleistungen bei Störungen in den internen Kommunikationssystemen erwartet werden können.[474]

Im Rahmen der Vertrauensschadenversicherung, die den Versicherungsnehmer, fast immer ein Unternehmen, gegen von eigenen schadenersatzpflichtigen Mitarbeitern verursachte Vermögensschäden schützt, stellt die Computer-Mißbrauch-Ver-

473 Die TELA Versicherung empfiehlt Versicherungssummen, die gemäß der Festplattenspeicherkapazität festgelegt werden. Vgl. TELA Versicherung (1994).

474 Vgl. dazu Deutscher Versicherungs-Schutzverband (1992), S. 22ff.

sicherung eine Teilversicherung dar.[475] Sie ist auf Versicherungsfälle begrenzt, welche die Mitarbeiter des Versicherungsnehmers durch die vorsätzliche, rechtswidrige Bereicherung an den Vermögenswerten des Versicherungsnehmers oder durch deren Beeinträchtigung mittels Manipulation oder Zerstörung von Datenträgern und Datenverarbeitungsanlagen verursachen. Zwar muß der Schädiger namentlich identifiziert werden, um die Entschädigungsleistung zu erhalten, jedoch kann der Versicherungsschutz auf nicht identifizierbare Schadenstifter und auf außenstehende Dritte ausgedehnt werden, wobei in solchen Schadensfällen nur eine rechtswidrige Bereicherung an Vermögenswerten und nicht eine vorsätzliche Schädigung des Versicherungsnehmers abgedeckt wird. Dienstleistungsbetriebe der Datenverarbeitung können zusätzlich Versicherungsschutz für Vermögensschäden ihrer Kunden erhalten. Die Entschädigungsleistung erstreckt sich bei bereicherungsmotivierten Schadensfällen jedoch nur auf rechtswidrig erlangte Geldbeträge oder Vermögenswerte des Versicherungsnehmers und seiner Kunden. Folgeschäden durch den Verrat vertraulicher Betriebsdaten an einen Mitbewerber des Versicherungsnehmers in Form von Umsatzeinbußen werden nicht entschädigt. Bei vorsätzlich motivierten Schadensfällen ohne Bereicherungsmotiv ersetzt der Versicherer lediglich die Kosten zur Wiederherstellung des ursprünglichen Zustandes vor der Verletzung der Informationssicherheit.

Bei der Verarbeitung und Übermittlung personenbezogener Daten kann es zu Verletzungen von Vorschriften des Bundesdatenschutzgesetzes BDSG[476] kommen, für dadurch verursachte Vermögensschäden können die Datenverarbeiter im Sinne des BDSG von Dritten haftpflichtig gemacht werden. Dagegen kann der Versicherungsnehmer einschließlich seiner Bediensteten zusätzlich zur allgemeinen Haftpflichtversicherung für Vermögensschäden eine Daten-Haftpflichtversicherung abschließen, um die dabei entstehenden Vermögensschäden abzudecken. Hierbei sind jedoch nicht Personen- und Sachschäden eingeschlossen, sondern lediglich Haftpflichtansprüche auf Ersatz eines immateriellen Schadens wegen Verletzung von Persönlichkeitsrechten. Die Versicherungsleistung besteht also darin, daß der Versicherer den Versicherungsnehmer von den erhobenen Ansprüchen Dritter befreit, indem er bei gerechtfertigten Ansprüchen den Haftpflichtschaden ersetzt und bei unbegründeten Ansprüchen diese eventuell auf dem Rechtswege zurückweist.[477]

---

475 Vgl. dazu die ausführliche Darstellung von Heidinger (1980).

476 Vgl. BGBl. S. 2954 vom 20. 12. 1990.

477 Die Betreiber von Kommunikationssystemen können sich durch eine Software-Haftpflichtversicherung, vgl. Schulze Schwienhorst (1995), gegen Entschädigungsforderungen von

Schließlich können Datenverarbeiter im Sinne des BDSG eine Daten-Rechtsschutzversicherung abschließen, um die Kosten, die bei der gerichtlichen Abwehr von Ansprüchen Betroffener und des Vorwurfes einer Straftat oder Ordnungswidrigkeit nach dem BDSG entstehen, auf den Versicherer zu überwälzen.

Aus der Übersicht über die bestehenden Versicherungsmöglichkeiten für die Informationssicherheitsrisiken von Kommunikationssystemen können folgende Schlüsse gezogen werden. Erstens richten sich die Versicherungsangebote i. d. R. nicht an Privatpersonen, sondern an Unternehmen und im Fall der Daten-Haftpflichtversicherung auch an öffentliche Stellen, weil letztere im Schadensfall im Gegensatz zu privaten Teilnehmern, welche vor allem immaterielle Beeinträchtigungen erfahren, einen beträchtlichen Vermögensverlust zu verzeichnen haben und deshalb auch bereit sind, die relativ hohen Prämien zu bezahlen. Die Eingrenzung des Versichertenkreises auf Unternehmen hängt deshalb unmittelbar mit der Beschränkung der Entschädigungsleistungen durch die Versicherer auf materielle Vermögensverluste zusammen. Zweitens werden neben dem Ersatz der Hardware durch die Elektronik-Versicherung bei der Beeinträchtigung der Informationssicherheit lediglich die Kosten ersetzt, die bei der Wiederherstellung der Verfügbarkeit und der Integrität der Datenbestände und der Stornierung nicht rechtmäßiger Kommunikationsprozesse und einer dadurch bedingten Betriebsunterbrechung anfallen. Vermögensverluste aufgrund von Vertraulichkeitsverletzungen, wie die Weitergabe betriebswichtiger Daten, werden nicht versichert. Schließlich ist offensichtlich geworden, daß sich das bestehende Versicherungsangebot vor allem auf die Schadensfälle bezieht, die im Endgerätebereich der Kommunikationsteilnehmer lokalisiert werden können. Für Risiken während Transferierung von Daten auf offenen Kommunikationsnetzen oder durch den Zugriff unbekannter Dritter auf interne Datenbestände mittels Kommunikationsverbindungen wird erst seit wenigen Jahren ein eingeschränkter Versicherungsschutz durch die erweiterte Software- oder Computer-Mißbrauch-Versicherung angeboten.

Die vorangegangene Übersicht hat also deutlich gemacht, daß nur bestimmte Informationssicherheitsrisiken, die durch die Nutzung von Kommunikationssystemen hervorgerufen werden, von den deutschen Versicherungsunternehmen versichert werden.[478] Ob daraus ein staatlicher Handlungsbedarf abgeleitet werden darf, gilt

---

Teilnehmer schützen, deren Informationssicherheit durch Fehler der Systemsoftware geschädigt werden.

478 Auch das Versicherungsangebot in den Vereinigten Staaten ist bzgl. Computerrisiken unvollständig. Vgl. dazu System Security Study Committee u. a. (1991), S. 174ff.

es im nächsten Abschnitt unter Bezugnahme auf die diskutierten Bedingungen der Versicherbarkeit und die Analyse der Versicherungsnachfrage zu klären.

2.5.5.6 Potentielle Gründe für einen staatlichen Eingriff in den Versicherungsmarkt für Informationssicherheitsrisiken

Wie im vorangegangenen Abschnitt gezeigt wurde, ist das Versicherungsangebot bezüglich der Risiken von Kommunikationsnetzen lückenhaft. Ob und in welcher Form dieser unvollständige Versicherungsschutz durch staatliche Eingriffe erweitert werden sollte, ist Gegenstand dieses abschließenden Abschnittes zur Versicherungsmöglichkeit von Informationssicherheitsrisiken offener Kommunikationssysteme.

Hinsichtlich des Kreises der Versicherungsnehmer ist deutlich geworden, daß sich das Versicherungsangebot lediglich an Unternehmen und nicht an Privatpersonen richtet. Diese Eigenheit kann jedoch dadurch erklärt werden, daß private Kommunikationsteilnehmer im Schadensfall weniger materielle Vermögensschäden, sondern vor allem immaterielle Schäden davontragen und, wie in Abschnitt 2.5.5.4 gezeigt, für letztere nach der Erwartungsnutzenmaximierung keine Versicherungsnachfrage besteht. Die Begrenzung der Versicherungsnehmer auf Unternehmen oder öffentliche Institutionen stellt also aus allokativen Gründen keinen Handlungsbedarf für einen staatlichen Eingriff hinsichtlich der Ausweitung des Versichertenkreises auf Privatpersonen dar.

Die Deckung von Vermögensschäden konzentriert sich neben der Elektronik-Versicherung zur Entschädigung von Hardwareschäden vor allem auf die Fälle, die durch die unmittelbare Zerstörung oder Veränderung von Daten oder durch die daraus verursachten und objektiv quantifizierbaren Folgeschäden anfallen. Materielle Risiken durch die Verletzung der Vertraulichkeit von Daten und Kommunikationsinhalten werden nicht abgedeckt. Die ökonomische Begründung dafür liegt nicht in einer fehlenden Versicherungsnachfrage, sondern in der begrenzten Fähigkeit der Versicherungsanbieter, die erwarteten Schadenhöhen und daraus abgeleitet faire Versicherungsprämien korrekt zu berechnen. Denn selbst bei den Schäden, die durch die Wiederherstellung von Daten und durch die Stornierung unrechtmäßiger Kommunikationsprozesse rückgängig gemacht werden können, besteht eine starke Unsicherheit bei der Kalkulation erwarteter Schadensausmaße. Jedoch dienen in diesen Fällen die voraussichtlich anfallenden Reparaturkosten und eine Entschädigungsobergrenze als Strategien zur Reduzierung der negativen Folgen von Berech-

nungsfehlern, so daß die Bedingungen der Versicherbarkeit erfüllt sind.[479] Bei Verletzungen der Vertraulichkeit von in offenen Kommunikationssystemen übermittelten Informationen handelt es sich um irreparable Schäden, die unkalkulierbare und in vielen Fällen auch nicht objektiv nachweisbare Folgen nach sich ziehen, so daß damit zwei wesentliche Bedingungen für die Versicherbarkeit nicht erfüllt sind.[480] Jedoch stellt auch diese Begrenzung des Versicherungsangebotes keine Veranlassung zu einem staatlichen Eingriff dar, weil es einer staatlichen Institution auch nicht möglich ist, eine genauere Kalkulation der Erwartungsschäden durchzuführen und eingetretene Vermögensschäden objektiv nachzuweisen.

Abschließend gilt es zu untersuchen, warum sich der Versicherungsschutz nur bedingt auf die bei den eigentlichen Kommunikationsvorgängen auftretenden Informationssicherheitsrisiken bezieht, während potentielle Schäden bei isolierten Datenverarbeitungsanlagen und -beständen umfassend abgedeckt werden. Die Ursache liegt in der Besonderheit des Transportes von Informationen. Zum einen liegen bei Kommunikationsprozessen in offenen Netzen zwischen Sender und Empfänger eine Reihe von Leitungen und Vermittlungsstellen, die es im Schadensfall u. U. unmöglich machen, den Ort oder die Komponente des Kommunikationssystems, der den Schadensfall verursacht, zu bestimmen. Diese Lokalisierung bzw. Konkretisierung der Schadensursache aber bildet für den Versicherer die Basis für die Kalkulation der Schadenswahrscheinlichkeiten und damit auch der Versicherungsprämien. Zum anderen besteht gerade bei Kommunikationsvorgängen die Gefahr, daß die Vertraulichkeit der Kommunikationsinhalte verletzt wird, ohne daß dies vom Versicherungsnehmer objektiv nachgewiesen werden kann. Dies bedeutet für den Versicherten, daß er nur in einem Bruchteil der Schadensfälle eine Entschädigung von der Versicherung zu erwarten hat und damit der Abschluß einer Versicherung aus wirtschaftlichen Gesichtspunkten nicht zu empfehlen ist. Selbst wenn es zukünftige Kommunikationssysteme ermöglichen, den Eintritt und die Ursache von Schadensfällen exakter zu identifizieren, führt die Vernetzung in sehr leistungsfähigen Kommunikationssystemen zu einer Abhängigkeit bzw. Korrelation der Einzelrisiken. So betrifft der Ausfall einer Vermittlungsstelle unmittelbar eine Vielzahl

---

479 Ex post Moral Hazard ist auch nicht möglich, da lediglich nachgewiesene Reparaturkosten ersetzt werden oder der Versicherer die Schäden selbst repariert, und zu ex ante Moral Hazard bestehen nur begrenzt Anreize, da lediglich materielle Schäden kompensiert werden, so daß Nutzeneinbußen durch immaterielle Schädigungen bestehen bleiben.

480 Der Verlust der Vertraulichkeit wird gerade durch den generellen öffentlichen Gutscharakter von Informationen möglich, und der daraus anfallende Schaden ist aus demselben Grund nicht beweis- und quantifizierbar und deshalb auch nicht versicherbar.

von Kommunikationsbeziehungen[481], die dann gleichzeitig beim Versicherer als Schadensfall gemeldet werden und damit zu Entschädigungsforderungen in katastrophalem Ausmaße führen. Deshalb zögern die Versicherungsunternehmen, Risiken offener Kommunikationssysteme abzudecken.[482]

Letztlich kann nur diese Eigenschaft der Informationssicherheitsrisiken offener Kommunikationssysteme einen staatlichen Eingriff in den Versicherungsmarkt rechtfertigen. Als Lösungsmöglichkeiten bieten sich grundsätzlich die generelle Versicherungspflicht aller Kommunikationsteilnehmer oder die Einrichtung einer staatlichen Versicherung an. Im ersten Fall werden alle Teilnehmer dazu verpflichtet, ihre Informationssicherheitsrisiken zu versichern, wobei die Wahl der Versicherungsgesellschaft, wie bei der Kfz-Haftpflichtversicherung, freigestellt bleibt. Jedoch ist offensichtlich, daß die nicht erfüllte Unabhängigkeit der Einzelrisiken auch durch diese Form der Versicherungspflicht immer noch besteht und damit einer wesentlichen Bedingung der Versicherbarkeit durch einen privaten Anbieter nicht genügt wird. Deshalb bleibt als zweite Möglichkeit eine staatliche Zwangsversicherung nach dem Prinzip der Arbeitslosenversicherung, welche alle Kommunikationsteilnehmer dazu verpflichtet, sich bei einer gesetzlichen Versicherung zu versichern. Dadurch wird ein Poolen der Risiken von Teilnehmern verschiedener Kommunikationssysteme erreicht, so daß zumindest eine gewisse Unabhängigkeit der Teilnehmergruppenrisiken gegeben ist. Außerdem kann eine Staatsversicherung durch den Rückgriff auf finanzielle Quellen des Staatshaushaltes katastrophale Schadensfälle verkraften. Es stellt sich ferner noch die Frage nach einer adäquaten Bemessungsgrundlage zur Berechnung der Prämien. Hinsichtlich der Schadenhöhe kann im kommerziellen Bereich der Umsatz eines Unternehmens unter Berücksichtigung der Intensität der Kommunikationsaktivitäten dienen. Eine Differenzierung der Teilnehmer nach Schadenswahrscheinlichkeiten ist innerhalb eines Kommunikationssystems aufgrund des gemeinsamen Informationssicherheitsstandard eigentlich nicht notwendig. Sind aber sicherheitsfördernde Maßnahmen im Endgerätebereich möglich, dann sollte - wie es bereits in der Praxis geschieht - eine Differenzierung der Prämien erfolgen. Ebenfalls sollten Teilnehmern aus Kommunikationssystemen mit verschiedenen Informationssicherheitsmecha-

---

481 So verhinderte 1990 der neunstündige Ausfall der New Yorker und anderer zentraler Schaltstellen von AT&T ungefähr 40 Millionen Telefonverbindungen. Vgl. Lütge (1995), S. 19.

482 In dieser Betrachtung wurde von der Produkthaftung der Betreiber von Kommunikationsnetzen und -diensten abstrahiert. Diese führt, wie in Abschnitt 2.7.3 gezeigt wird, zwar dazu, daß die Geschädigten Ansprüche an die Betreiber stellen werden, ändert jedoch nichts an der Versicherungsproblematik, weil auch letztere von einem privaten Versicherer nur bedingt Versicherungsschutz für ihre Risiken erhalten werden.

nismen entsprechend unterschiedliche Prämien abverlangt werden. Privatpersonen müssen nach den erwartungsnutzentheoretischen Ergebnissen aus Abschnitt 2.5.5.4 von der Versicherungspflicht freigestellt werden, insofern die Informationssicherheitsrisiken von Kommunikationssystemen lediglich ihre immateriellen Nutzenkomponenten bedrohen. Denjenigen, die materielle Vermögensverluste fürchten, sollte eine freiwillige Versicherungsmöglichkeit eingeräumt werden.

Eine staatliche Zwangsversicherung kann grundsätzlich auch noch dazu dienen, meritorische Ziele zu realisieren, die ihre Berechtigung durch irrationales oder uninformiertes Verhalten der Kommunikationsteilnehmer erfahren.[483] Diese werden deshalb ähnlich wie bei der Alters- oder Unfallvorsorge dazu neigen, gegen ihre Informationsrisiken keinen oder einen nur unzureichenden Versicherungsschutz nachzufragen.[484] Der Versicherungszwang kann teilweise Abhilfe schaffen, indem im Schadensfall zumindest ein Grundversicherungsschutz eingeräumt wird. Falls man dagegen den Betreibern von Kommunikationsnetzen und -diensten rationales Verhalten unterstellt, dann werden diese sowohl ein effizientes Niveau an Informationssicherheitsmaßnahmen in ihren Kommunikationssystemen als auch einen ausreichenden Versicherungsschutz realisieren.

Im folgenden Kapitel werden Gründe aufgezeigt, warum hinsichtlich der Informationssicherheit in offenen Kommunikationssystemen zu erwarten ist, daß die in diesem Kapitel abgeleiteten Effizienzbedingungen selbst in einem von Wettbewerbsmechanismen dominierten Markt durch die private Initiative der Wirtschaftssubjekte nicht erfüllt werden können.

---

[483] Molitor (1987), S. 423, bezeichnet auch die staatliche Arbeitslosenversicherung als Meritorisierungsinstrument, obwohl die alleinige Abhängigkeit individueller Risiken eigentlich noch keinen meritorischen Bedarf auslöst.

[484] Dafür spricht der Vergleich zwischen der Häufigkeit tatsächlich eingetretener Risiken und den individuellen Einschätzung nach Prioritäten in Näther (1991), S. 81, der erhebliche Diskrepanzen offenbart.

2.6 Ursachen von Allokationsineffizienzen hinsichtlich der Informationssicherheit in Kommunikationsnetzen und -diensten

2.6.1 Vorbemerkungen

Nachdem in Kapitel 2.5 das effiziente Ausmaß an Informationssicherheit in Kommunikationsnetzen und -diensten in Abhängigkeit von der Teilnehmerzahl n* und dem Integrationsgrad I* theoretisch bestimmt worden ist, werden in diesem Kapitel konkrete Ursachen identifiziert, die zu einem suboptimalen Sicherheitsniveau in Kommunikationsnetzen führen können. Hierbei werden die allgemeinen Gründe für Allokationsineffizienzen auf Märkten für Sicherheitsgüter nicht noch einmal aufgenommen, sondern es wird auf Kapitel 1.4 des ersten Teils der Arbeit verwiesen, wenn diese keine konkreten Anknüpfungspunkte für die Informationssicherheit in Kommunikationsnetzen bieten. Deshalb erfolgt eine Konzentration unter der Vernachlässigung des irrationalen Verhaltens unter Unsicherheit auf die beiden Ursachenkomplexe unvollständige und asymmetrische Informationsverteilung und externe Effekte, wobei diese jeweils nochmals in Teilaspekte differenziert werden.[485]

Eine weitere Einschränkung wird dahingehend vorgenommen, daß vor allem Gründe für einen allgemeinen Verbraucher- bzw. Kommunikationsteilnehmerschutz und nicht für den Datenschutz i. e. S. im Bereich der Telekommunikationsnutzung identifiziert werden sollen.[486] Dies bedeutet konkret, daß telekommunikationsbedingte Risiken für das Grundrecht auf informationelle Selbstbestimmung[487] wie Gefahren durch das Eindringen in die Privatsphäre, durch die Profilbildung mittels der Auswertung von Kommunikationsbeziehungen, durch die Zweckentfremdung erhobener Nutzerdaten und der Überwachung des Nutzerverhaltens nicht weiter analysiert werden. Es wird sich weiterhin auf den allgemeinen Begriff der Informationssicherheit beschränkt. Ferner bleiben die generelle Versorgung aller Gesellschaftsmitglieder mit informationssicheren Kommunikationssystemen und die allgemeine Auswirkungen auf das politisch-gesellschaftliche System unberücksichtigt.[488] Die Aufmerksamkeit richtet sich also ausschließlich auf die allokativen Probleme der bereits diskutierten Risiken der Informationssicherheit bei Kommunikationsprozessen, nämlich auf die Gefahren für die

---

485 Es wird nicht noch einmal auf die potentiellen Ineffizienzen des Versicherungsmarktes eingegangen. Vgl. dazu Abschnitt 2.5.5.

486 Vgl. zur Unterscheidung Ungerer (1993), S. 28ff.

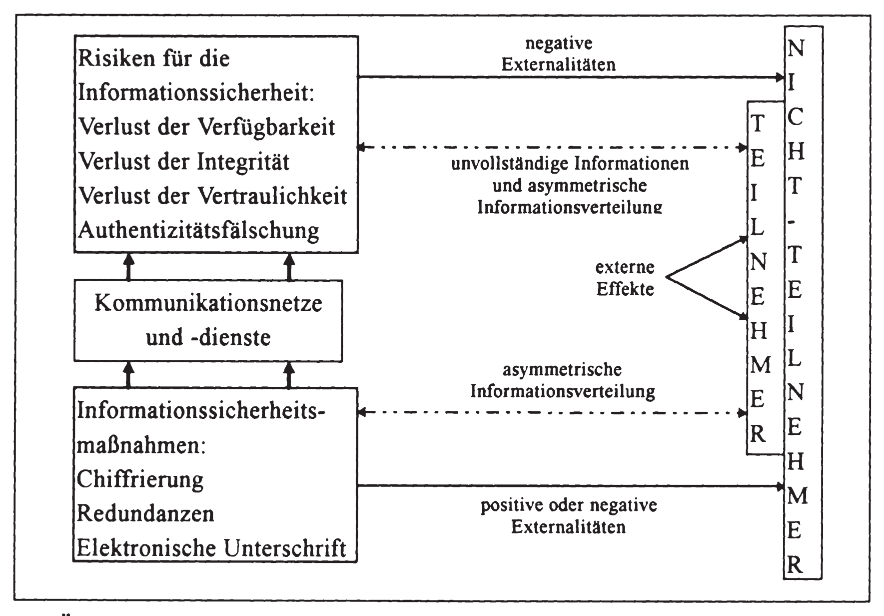
487 Vgl. dazu Garstka (1993), S. 32f.

488 Vgl. dazu Groebel (1994), S. 78, und o. V. (1995), S. 3.

Verfügbarkeit, Integrität und Vertraulichkeit der Kommunikationsinhalte und der Identitäts- bzw. Authentizitätsfälschung.

Ferner werden reine angebotsbegründete Ursachen von Allokationsineffizienzen nicht weiter problematisiert, denn die allgemeine Analyse des Angebots an Sicherheitsmaßnahmen in Kapitel 1.3 hat deutlich gemacht, daß Fehlallokationen für gewöhnlich nur in Zusammenhang mit Unvollkommenheiten auf den Märkten der Basisgüter - hier der Kommunikationsnetze und -dienste - auftreten. Die Angebotsstrukturen dieser Märkte werden in dieser Arbeit nicht weiter auf mögliche Unzulänglichkeiten untersucht, weil dem zukünftigen Regulierungsrahmen des Telekommunikationsmarktes in der Bundesrepublik Deutschland entsprechend Wettbewerb unterstellt wird.[489]

Die folgende Übersicht 10 macht deutlich, wo asymmetrische bzw. unvollständige Informationsverteilungen und Externalitäten potentiell vorliegen können.



Übersicht 10: Unvollständige Informationen, asymmetrische Informationsverteilungen und externe Effekte

489 Vgl. dazu das Eckpunkte-Papier des Bundesministeriums für Post und Telekommunikation (1995) über den künftigen Regulierungsrahmen im Telekommunikationsbereich.

In den nachfolgenden Abschnitten werden die verschiedenen Arten asymmetrischer Informationsverteilung und die möglichen Ursachen von Externalitäten darauf untersucht, ob sie so gravierende Abweichungen vom in Kapitel 2.5 abgeleiteten Optimum verursachen können, welche den Einsatz verschiedener, in Kapitel 2.7 dargestellter, staatlicher Instrumente verlangt.

2.6.2 Unvollständige Informationen, asymmetrische Informationsverteilungen und daraus resultierende Allokationsineffizienzen

2.6.2.1 Unvollständige Informationen über die Bedrohungen durch Verletzungen der Informationssicherheit

In Kapitel 2.5 hat sich gezeigt, daß aus allokativer Effizienz bei Unterstellung stetiger Grenzkosten- und Grenznutzenverläufe solange Maßnahmen zur Informationssicherheit ergriffen werden sollen, bis ein Ausgleich von Grenznutzen und Grenzkosten erreicht ist.[490] Für das Erreichen dieses Optimums ist es jedoch erforderlich, genaue Kenntnisse über die einzelnen Komponenten des Grenznutzens zu haben. Dies kann aber daran scheitern, daß die notwendigen Informationen darüber unzureichend sind. Es wird deshalb zu untersuchen sein, ob dies hinsichtlich der Risiken und Maßnahmen der Informationssicherheit der Fall ist.

Die Risiken für die Informationssicherheit können zum einen hinsichtlich ihrer Teilkomponenten unterschieden und zum anderen nach potentieller Schadenhöhe L bzw. Nutzeneinbuße IM und Schadenswahrscheinlichkeit p differenziert werden. Im folgenden wird nach letzterer Unterscheidung vorgegangen, wobei die Einzelkomponenten der Informationssicherheit besonders berücksichtigt werden.

In einem ersten Schritt soll deshalb untersucht werden, ob die Benutzer von Kommunikationsnetzen ausreichende Kenntnisse über die Schadenpotentiale - verursacht durch die Verletzung der Informationssicherheit - haben und damit diese Komponente des Grenznutzens der Informationssicherungssysteme adäquat einzuschätzen vermögen. Es handelt sich also genaugenommen zum einen um die Problematik, daß die Kommunikationsteilnehmer sich nur unzureichend über ihre Wertschätzung einer si-

---

490 In der Notation des Kapitels 2.5 handelt es sich um die Effizienzbedingungen (39′) und (40′).

cheren Übermittlung der Kommunikationsinhalte bewußt sind.[491] Zum anderen ist eine asymmetrische Informationslage zwischen Benutzern und den Netz- und Diensteanbietern in dem Sinne vorhanden, daß letztere vor allem hinsichtlich der Vielfalt von Schadensmöglichkeiten und der Schadeneintrittswahrscheinlichkeit, deren Abschätzungsproblematik in einem zweiten Schritt behandelt wird, einen Informationsvorsprung haben. Jedoch ist auch die Anbieterseite Unsicherheiten ausgesetzt, da Umfang und Art exogener Bedrohungen ex ante nur begrenzt abzuschätzen sind.[492]

Findet eine Verletzung der Informationssicherheit innerhalb des Kommunikationssystems statt, dann kann dies für die Betroffenen - also Sender und/oder Empfänger - sowohl materielle Vermögensverluste als auch immaterielle Nutzeneinbußen mit sich bringen. Bei Verletzungen der Verfügbarkeit, der Integrität der Inhalte und Authentifikationsmanipulationen ist zumindest ex post das Schadensausmaß weitgehend bestimmbar und kann damit als Orientierungsgröße für die Einschätzung potentieller zukünftiger materieller Schäden herangezogen werden. Beeinträchtigungen der Vertraulichkeit ziehen Schäden nach sich, die auch ex post nur unvollständig aufzudecken sind, so daß die Extrapolation vergangener Schäden nur mit Vorsicht als Anhaltspunkt für zukünftige Schadensausmaße dienen kann. Diese Problematik verschärft sich noch für die Fälle, in denen keine materiellen Schäden, sondern lediglich individuelle immaterielle Nutzeneinbußen auftreten, weil diese, wie sich vor allem in Abschnitt 2.5.5 über die Versicherbarkeit gezeigt hat, als unterschiedlich intensiv empfunden werden und damit eine monetäre Quantifizierung wenig Aussagegehalt hat. Insgesamt läßt sich also festhalten, daß die Unsicherheit des einzelnen Teilnehmers über das ihn bedrohende Schadenpotential aufgrund seiner fehlenden objektiven Bewertbarkeit und seiner Abhängigkeit vom jeweiligen Schadensfallszenario nur durch eigene Erfahrungswerte oder gezielte Informationsbeschaffung abzubauen ist. Dadurch können zwar auch Allokationsineffizienzen ausgelöst werden, die im weiteren jedoch nur dann berücksichtigt werden, wenn sie gleichzeitig durch Informationsasymmetrien gegenüber der Angebotsseite verursacht worden sind. Denn mittels der Abstraktion irrationalen Verhaltens werden alle Teilnehmer an Kommunikationssystemen ihr Informationsdefizit hinsichtlich der Wertschätzung über ihre eigenen Kommunikationsinhalte auf ein effizientes Maß reduzieren.

---

[491] Zwar unterliegen die Kommunikationsteilnehmer einer gewissen Nutzenunkenntnis bzgl. der transportierten Kommunikationsinhalte, jedoch kann davon ausgegangen werden, daß die Netz- und Diensteanbieter darüber noch weniger Kenntnisse haben und damit eine gewisse Informationsasymmetrie zugunsten der Teilnehmer vorliegt.

[492] Die Trennung zwischen Anbieter und Kommunikationsteilnehmer steht nicht im Gegensatz zur Clubgüterbetrachtung eines Kommunikationsnetzes von Kapital 2.4, wenn man von einer Principal (= Gruppe der Kommunikationsteilnehmer)-Agent (=Anbieter)-Beziehung ausgeht.

Ferner ist es durchaus möglich, daß von den Kommunikationsteilnehmern nicht alle potentiellen Schadensarten erfaßt werden, während im Gegensatz dazu die Angebotsseite in diesem Fall zumindest für bereits in Betrieb befindliche Kommunikationssysteme einen Informationsvorsprung hat. Schließlich muß noch erwähnt werden, daß eine umfassende statistische Erfassung der Schadensfälle durch Verletzungen der Informationssicherheit in Kommunikationsnetzen nicht durchgeführt wird[493], während für den Straßenverkehr die Unfallstatistik ausführlich informiert.[494] Im ganzen ist deshalb festzustellen, daß sich die Kommunikationsteilnehmer nur bedingt der Schadenpotentiale der Informationssicherheit bewußt sind. Dies wird auch dadurch dokumentiert, daß über die Hälfte von 240 Datenverarbeitungsunternehmen, also professionellen Informationsverarbeitern, keine Angaben über den Schutzbedarf ihrer Anwendungen und Systeme hinsichtlich Informationssicherheit machen konnte und Informationssicherheitsmaßnahmen bei der Telekommunikation und der Datenfernübertragung im Vergleich zur zentralen Datenverarbeitung stark vernachlässigt werden.[495]

Es ist damit offensichtlich geworden, daß die Benutzer von Kommunikationsnetzen und -diensten über potentielle Schadensausmaße vor allem unvollständig informiert sind und ein Informationsvorsprung der Anbieterseite lediglich hinsichtlich der Vielfalt möglicher Risiken auszumachen ist. Berücksichtigt man die Differenzierung der Netze und Dienste nach ihrer Leistungsfähigkeit bzw. nach ihrem Integrationsgrad I*, so kann davon ausgegangen werden, daß mit der zunehmenden Komplexität sowohl der Grad unvollständiger Information der Teilnehmer bezüglich der Schadenhöhe als auch die asymmetrische Informationsverteilung über die verschiedenen Schadenskategorien zunehmen.

In der Fallstudie wurde von teilnehmerbezogenen Sicherheitsvorkehrungen aus Anschaulichkeitsgründen abstrahiert und ausschließlich auf Basis von Informationssicherheitsmechanismen, die innerhalb eines Kommunikationsnetzes und -dienstes allgemein installiert werden, argumentiert. Im folgenden Abschnitt wird die asymmetrische Informationsverteilung bezüglich der Effizienz der betrachteten Informationssicherheitsmechanismen und der damit unmittelbar zusammenhängenden Schadenswahrscheinlichkeiten gemeinsam analysiert, weil mit der Wahl für ein Kommunikationssystem gleichzeitig das herrschende Informationssicherheitsniveau bestimmt wird.

---

493 Vgl. dazu auch System Security Study Committee u. a. (1991), S. 163f.

494 Vgl. Statistisches Bundesamt (1994), S. 354ff, wo die Straßenverkehrsunfälle nach Unfallbeteiligten, Unfallort und Unfallursachen differenziert werden.

495 Vgl. dazu die KES Sicherheitsstudie 1994 von Gartner & Konrad (1994), S. 7ff.

2.6.2.2 Asymmetrische Informationsverteilung hinsichtlich der Effizienz von Informationssicherheitssystemen und der Schadenswahrscheinlichkeiten

Während die Kommunikationsteilnehmer bezüglich der möglichen Schadensausmaße eher unvollständig informiert sind, liegt über die Schadenswahrscheinlichkeiten i. d. R. eine asymmetrische Informationsverteilung i. e. S. vor. Denn es kann davon ausgegangen werden, daß die Teilnehmer gegenüber den Netz- und Diensteanbietern darüber einen Informationsnachteil haben, wobei letztere auch nicht immer korrekt informiert sein müssen. Kann die Schadenswahrscheinlichkeit als durchschnittliche Anzahl von Schadensfällen innerhalb eines bestimmten Zeitraums oder pro Gesamtanzahl der Kommunikationsvorgänge innerhalb eines Kommunikationsnetzes oder -dienstes vom Betreiber bestimmt werden, dann hat der potentielle Teilnehmer ex ante vor dem Anschluß an ein Netz oder Dienst ein Informationsdefizit, weil die tatsächliche Zuverlässigkeit ohne Erfahrungswerte nicht abzuschätzen ist. Bezüglich der Problematik, die Schadenswahrscheinlichkeit von Verletzungen der Informationssicherheit in einem Kommunikationssystem richtig einzuschätzen, ist es analog zur Analyse der Versicherungsproblematik angebracht, verschiedene Schadenskategorien zu unterscheiden. Verletzungen der Verfügbarkeit und der Integrität von Kommunikationsverbindungen bzw. -inhalten sind ex post von den einzelnen Teilnehmern im allgemeinen festzustellen, während Authentifikationsmanipulationen nicht immer oder nur mit zeitlicher Verzögerung aufgedeckt werden und Vertraulichkeitsbeeinträchtigungen in vielen Fällen gänzlich unentdeckt bleiben.[496] Grundsätzlich werden Netz- und Diensteanbieter mit derselben Informationsproblematik konfrontiert, wobei diese zum einen auf einen längeren Erfahrungshorizont zurückblicken können und zum anderen einen Informationsvorsprung gegenüber den Kommunikationsteilnehmern bezüglich der Effizienz ihrer Informationssicherheitssysteme haben. Es kann hierbei eine Differenzierung nach Schadensursachen vorgenommen werden. Während ihre Einschätzung der rein technisch bedingten Störungsanfälligkeit (= safety-Eigenschaften) durch Testauswertungen relativ zuverlässig ist, können sie die Verletzlichkeit der Informationssicherheit gegenüber bewußten Angriffen[497] (= security-Eigenschaften) nur vage bestimmen. Denn intelligente Angreifer werden sich bemühen, die ex ante nicht immer offensichtlichen Schwachstellen der Informationssicherheitssysteme mit den sich im Zuge des technischen Fortschritts weiterentwickelnden Angriffsstrategien auszunutzen.[498]

---

[496] Die Schadensursache kann in der Praxis natürlich auch durch unzureichendes lokales oder teilnehmerinternes Sicherheitsmanagement begründet sein. Davon wird hier jedoch abgesehen.

[497] Vgl. zu den verschiedenen Angriffsformen Pohl & Weck (1993), S. 20f.

[498] Vgl. dazu auch Rosenbaum & Sauerbrey (1995), S. 31ff, die für eine weitere Unterscheidung in Angriffsversuchs- und Angriffserfolgswahrscheinlichkeiten eintreten.

Zwar baut sich das Informationsdefizit der Kommunikationsteilnehmer bezüglich der Schadenswahrscheinlichkeiten im Laufe der Nutzungszeit allmählich ab, jedoch verbleibt durch den Charakter der Zufallsereignisse und die Nichtentdeckung von Schadensfällen eine gewisse Restunsicherheit.

Soweit ist also festzustellen, daß sowohl potentielle als auch aktuelle Teilnehmer an Kommunikationsnetzen und -diensten gegenüber der Angebotsseite bezüglich der Schadenswahrscheinlichkeiten ein Informationsdefizit aufweisen.[499] Einschränkend muß bemerkt werden, daß auch Netz- und Dienstebetreiber aufgrund der unvollständigen Aufdeckung von Schadensfällen und der schwierigen Einschätzung des Potentials beabsichtigter Angriffe darüber keinen vollständigen, sondern nur einen begrenzten Kenntnisstand haben. Bedenkt man wiederum, daß die Schadenswahrscheinlichkeit mit der Teilnehmerzahl n^* und dem Integrationsgrad I^* eines Kommunikationsnetzes ansteigt, so führt zumindest letzterer zu einer zunehmenden Informationsasymmetrie zwischen Kommunikationssystem-Betreiber und -Nutzer, weil die damit verbundene zunehmende Komplexität des Kommunikationssystems von den Teilnehmern selbst ohne Hilfestellung nicht bewältigt werden kann.[500]

2.6.2.3 Allokationsineffizienzen aufgrund von Informationsasymmetrien

In den vorangegangenen Abschnitten wurde deutlich, daß die Kommunikationsteilnehmer ex ante sowohl unvollständig über ihre eigene Wertschätzung der Informationssicherheit informiert sind als auch gegenüber den Netz- und Dienstebetreibern einen Informationsnachteil hinsichtlich der Schadenswahrscheinlichkeiten haben und damit eine asymmetrische Informationsverteilung vorliegt. Da dieser Informationsstand kein exogener Parameter ist, sondern durch verschiedene Informationsstrategien der Anbieter- und Nachfragerseite endogenen Charakter hat, ist zu untersuchen, inwieweit dennoch Informationsdefizite bestehen bleiben und welche Arten von Allokationsineffizienzen daraus folgen.

Zunächst werden die Informationsbeschaffungsmöglichkeiten der Teilnehmer und somit die „Screening"-Strategien analysiert. Über den Erfahrungsaustausch mit ande-

---

[499] Darauf deutet auch die Diskrepanz zwischen antizipierter und aktueller Relevanz verschiedener Schadensursachen hin, wobei vor allem die Bedeutung irrtümlich begangener Fehler und technischer Defekte unterschätzt wird. Vgl. dazu die Gegenüberstellung bei Näther (1991), S. 81.

[500] So halten immerhin 29% der befragten Datenverarbeiter in der KES-Sicherheitsstudie 1994 ihre Kompetenz im Bereich Telekommunikation und Datenfernübertragung für verbesserungswürdig. Vgl. dazu Gartner & Konrad (1994), S. 9.

ren Teilnehmern kann das eigene Informationsdefizit ohne großen Aufwand zumindest teilweise abgebaut werden, wobei diese lediglich auf ihre individuellen Erfahrungen zurückgreifen können. Sind fundiertere Kenntnisse gefragt bzw. überfordert die Komplexität eines Systems mit einem hohen Integrationsgrad I* das begrenzte Verständnis der Teilnehmer, können Spezialisten in Anspruch genommen werden. Da vor allem die kommerziellen Kommunikationsteilnehmer sehr spezielle Rahmenbedingungen und Sicherheitsbedürfnisse haben, stellen die Beratungsleistungen für diesen Kundenkreis private Güter dar, so daß, wie die Praxis auch zeigt, sich private Informationssicherheitsspezialisten finden, die ihre Kenntnisse auf diesem Dienstleistungsmarkt anbieten.[501] Lediglich die Masse der Privatkunden, die auf den einzelnen Teilnehmer bezogen nur eine geringe Zahlungsbereitschaft für zusätzliche Kenntnisse über Informationssicherheit haben, wird damit konfrontiert, daß ihre Informationsbedürfnisse eher den Charakter eines öffentlichen Gutes haben und die Informationssicherheitsberater sich deshalb nicht alle Erträge ihrer Informationsgewinnungsbemühungen aneignen können. Die Folge ist, daß entweder in zu geringem Ausmaß oder zu einem weit über den Grenzkosten liegenden Preis allgemeine Informationen über die Risiken der Informationsunsicherheit und adäquate Sicherungsstrategien bereitgestellt werden.[502] Des weiteren muß mit gezielten Bestrebungen der Angebotsseite gerechnet werden, die Schwachstellen der Informationssicherheitssysteme ihrer Kommunikationsnetze und -dienste zu verbergen und das Bedrohungspotential zu verharmlosen.[503]

Trotz möglicher Verschleierungsstrategien von seiten der Netz- und Diensteanbieter gibt es für sie auch Anreize, die Qualität der Informationssicherheit in ihren Kommunikationssystemen den Nachfragern zu signalisieren, weil es sich hierbei um eine wichtige Kommmunikationsdienstleistungseigenschaft handelt.[504] Die direkten Werbestrategien[505] der Anbieter, die auf die ergriffenen Informationssicherheitsmechanismen und die dadurch reduzierten Schadenswahrscheinlichkeiten hinweisen, haben mit der fehlenden Akzeptanz durch die Nachfrager zu kämpfen. Denn eine schlechte Scha-

---

501 Die Studie von Frost & Sullivan (1992) prognostiziert für 1995 allein für die Beratungstätigkeiten in der Informationssicherheit einen Umsatz von 400 Millionen US$. Vgl. zu einer detaillierten Untersuchung des Leistungsangebotes von Sicherheitsberatern der Informationstechnik Voßbein (1994).

502 Vgl. Abschnitt 1.4.4 zu weiteren theoretischen Gründen für die Ineffizienz des Informationsmarktes.

503 Gerade bei wenigen Anbietern, wie es im Telekommunikationssektor im Moment der Fall ist, können sich „Schweigekartelle“ etablieren, die nach gemeinsamen Absprachen Informationen über Produktgefahren zurückhalten.

504 Vgl. dazu auch Büllesbach (1995), S. 6.

505 Eindrucksvollstes Beispiel war die Werbekampagne der Deutschen Telekom „Fünf Maßnahmen zum Schutz unserer Kunden und zum Kampf gegen die internationale Telefonkriminalität“ im Januar 1995 als Reaktion auf den Telefon-Sex-Skandal aus dem Herbst 1994.

densstatistik wird nicht preisgegeben, während die Nachfrager in Angaben, die auf eine hohe Verläßlichkeit eines Kommunikationssystems hindeuten, nur begrenzt Vertrauen haben, solange keine Mechanismen existieren, die Fehlinformationen sanktionieren können.

Erfolgsversprechender sind deshalb indirekte Signaling-Strategien. Die bei kurzlebigen Gütern und Dienstleistungen zu beobachtenden Reputationsstrategien[506] eignen sich bei Kommunikationsdienstleistungen insofern nicht unbedingt, weil der Anschluß an ein Kommunikationsnetz oder -dienst durch die Anschaffung von speziellen Endgeräten und die einmalig anfallenden Anschlußgebühren mit hohen Fixkosten verbunden ist und damit eine häufige Wiederholung der Nachfrageentscheidung nicht gegeben ist.[507] Falls sich durch den technischen Fortschritt und die Liberalisierung der Kommunikationsmärkte dieser Fixkostenblock vermindert und alternative Angebote offenstehen, dann ist der Wechsel von einem System, das die Erwartungen bezüglich der Informationssicherheit nicht erfüllt hat, durchaus möglich. Jedoch ist die Effizienz von Reputationsstrategien eingeschränkt, wenn die Nachfrager die Produkt- und Dienstleistungsqualität auch während des Nutzungszeitraumes nur begrenzt einzuschätzen vermögen, weil damit die Anbieter versuchen werden, ihren Gewinn durch qualitätsmindernde Einsparungen zu erhöhen. Diese Konstellation ist allerdings zum einen für Sicherheitssysteme allgemein[508] und zum anderen besonders für die Verletzungen der Vertraulichkeit von Kommunikationsinhalten gegeben, weil diese von den betroffenen Kommunikationsteilnehmern nur bedingt antizipiert werden, so daß Netz- und Diensteanbieter ihre Anstrengungen im Bereich der Informationssicherheit reduzieren können, ohne nach dem Eintreten von Schadensfällen unmittelbar der Gefahr des Nachfragerückgangs ausgesetzt zu sein.

Betrachtet man die Wahl eines Kommunikationsnetzes oder -dienstes als einmalige Nachfrageentscheidung des Teilnehmers, dann kommt für die Angebotsseite nicht die Reputation, sondern vor allem die Gewährung von Garantieversprechen als Signaling-Strategie in Frage. Jedoch ist dies auch nicht erfolgversprechend, weil die Anbieter aufgrund ihrer unvollkommenen Kenntnis des Bedrohungspotentials keine Garantie auf eine 100%-ige Gewährung der Informationssicherheit geben können und lediglich die Gewährleistung des Bemühens um die Informationssicherheit für die Nachfrager wenig

---

506 Vgl. dazu die Ausführungen in Abschnitt 1.4.4.

507 In der aktuellen Situation in der Bundesrepublik gibt es durch die Monopolstellung der Deutschen Telekom AG noch wenig Möglichkeiten, auf andere Netze- oder Dienste auszuweichen.

508 Vgl. dazu die Ausführungen in Abschnitt 1.4.4.

überzeugend ist.[509] Überdies werden in Schadensfällen die Betroffenen damit konfrontiert werden, die Schadensverursachung dem Netz- oder Dienstbetreiber nachweisen und eine dem Schaden entsprechende Kompensation einfordern zu müssen, was in sehr komplexen Kommunikationssystemen und bei Vertraulichkeitsverletzungen nur bedingt erfolgreich sein wird.

Die vorangegangene Diskussion hat gezeigt, daß selbst unter Berücksichtigung der marktinternen Strategien zum Abbau von Informationsasymmetrien bezüglich der Risiken für die Informationssicherheit in Kommunikationsnetzen die Kommunikationsteilnehmer weiter unter einem Informationsdefizit leiden, was die Angebotsseite ausnutzen wird, indem sie weniger als das volkswirtschaftlich effiziente Informationssicherheits- bzw. Self-protection-Niveau in den Kommunikationsnetzen implementieren wird. Durch den Prozeß der adversen Selektion wird es damit für einzelne Netz- und Diensteanbieter unmöglich, Nachfrager mit einer zusätzlichen Zahlungsbereitschaft für die Gewährleistung einer verbesserten Informationssicherheit in ihren Netzen und bei ihren Diensten zu finden, so daß sich ein Angebot in diesem Qualitätssegment nicht durchsetzen wird. Es wird sich deshalb lediglich ungefähr das Informationssicherheitsniveau einstellen, das dem von den Nachfragern antizipierbaren Grenznutzen der Informationssicherheitsmaßnahmen entspricht, weil ein geringeres Niveau durch Nachfragerückgang sanktioniert, aber ein höheres nicht mit einer größeren Zahlungsbereitschaft trotz höherer Kosten belohnt wird.[510] Dies wird in Abbildung 19, die auf die in Kapitel 2.5 getroffenen Annahmen zurückgreift, durch die Differenzierung in antizipierten und tatsächlichen Grenznutzen von Self-protection-Maßnahmen zur Sicherung der Informationssicherheit verdeutlicht. Außerdem wird das Ausmaß der Differenz zwischen dem volkswirtschaftlich effizienten Self-protection-Ausmaß r^*_{privat} und tatsächlich realisiertem Informationssicherheitsniveau mit der Teilnehmerzahl n^* und dem Integrationsgrad I^* ansteigen, weil die zunehmende Größe und die steigende Komplexität sowohl die Informationsasymmetrien in der Ausgangslage verschärfen als auch die Effektivität der Screening- und Signaling-Strategien begrenzen, so daß die verbleibende asymmetrische Informationsverteilung (ASI) zunimmt. Der aus den Informationsasymmetrien resultierende gesamtwirtschaft-

---

509 Vgl. dazu die Ausführungen in Abschnitt 1.4.4.

510 Die verschiedenen Anbieter von Kommunikationsnetzen oder -diensten werden also nur die durchschnittlich im Markt angebotene und von den Teilnehmern antizipierbare Informationssicherheit bereitstellen. Dagegen ist für leichter erfahrbare Leistungseigenschaften von Kommunikationssystemen, wie Funktionalität und Übertragungsgeschwindigkeit, eine positive Zahlungsbereitschaft vorhanden, so daß sich hier eine Vielfalt verschiedener Qualitätsniveaus, deren Durchschnittsqualität höher ist als bei Informationsasymmetrie, am Markt auch dauerhaft etablieren kann. Vgl. dazu auch System Security Study Committee u. a. (1991), S. 159.

liche Wohlfahrtsverlust, der sich aus dem zu niedrigen Ausmaß an Self-protection r'_{privat} und damit auch zu geringem Informationssicherheitsniveau ergibt, wird stilisiert durch das grau schraffierte Dreieck beschrieben.[511]

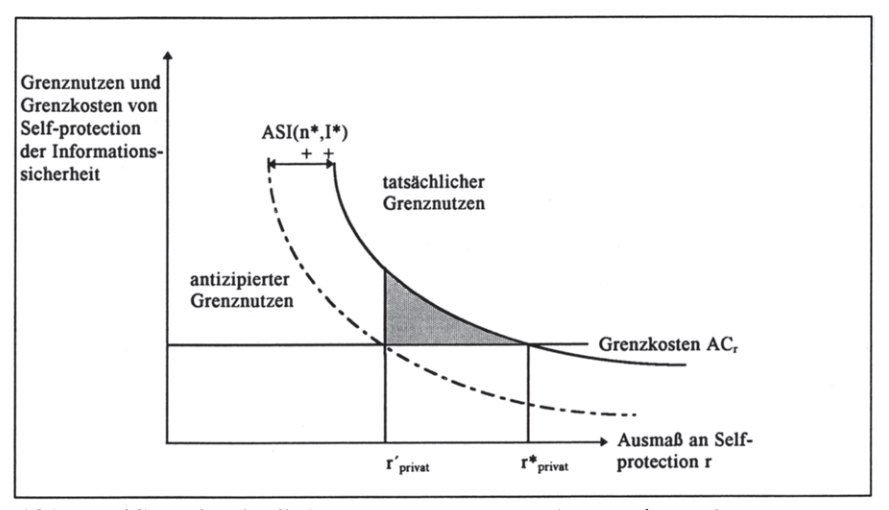


Abb. 19: Allokationsineffizienzen durch asymmetrische Informationsverteilung

In Kapitel 2.7 werden verschiedene wirtschaftspolitische Instrumente danach untersucht, inwieweit sie zum Abbau der Informationsasymmetrie und damit auch des Wohlfahrtsverlustes beitragen können und welche distributiven und fiskalischen Effekte damit einhergehen. Davor gilt es indes noch Externalitäten als zweite potentielle Ursache von Allokationsineffizienzen hinsichtlich Informationssicherheitsmaßnahmen zu untersuchen.

---

511 Bei neu einzuführenden Kommunikationsnetzen und -diensten kann Marktversagen auch dadurch ausgelöst werden, daß potentielle Nachfrager die damit verbundenen Risiken überbewerten und die Effektivität der implementierten Sicherheitsmaßnahmen unterschätzen und somit überhaupt keine Nachfrage entfalten.

2.6.3 Externe Effekte von Verletzungen der Informationssicherheit in Kommunikationsnetzen und -diensten

2.6.3.1 Externalitäten zwischen den Kommunikationsteilnehmern

Während sich bei der Analyse der asymmetrischen Informationsverteilung[512] auf die Beziehungen zwischen den Netz- und Dienstebetreibern und den Kommunikationsteilnehmern konzentriert wurde, wird in der Untersuchung der externen Effekte von Verletzungen der Informationssicherheit der Schwerpunkt zum einen auf das interne Verhältnis zwischen den Kommunikationsteilnehmern und zum anderen auf die externen Folgen für nur mittelbar betroffene Nicht-Teilnehmer gelegt.[513] Auf die Unterscheidung in die negativen Externalitäten der Risiken für die Informationssicherheit und in die positiven Externalitäten der Informationssicherheitsmaßnahmen in Kommunikationssystemen wird nur dann eingegangen, wenn zusätzliche Erkenntnisse gewonnen werden können, weil sich, wie in Abschnitt 1.4.5 gezeigt, die jeweiligen Folgen für die Allokationseffizienz qualitativ nicht unterscheiden.

Um die Beziehungen zwischen Kommunikationsteilnehmern auf technologische Externalitäten zu untersuchen, bietet sich folgende Differenzierung an. Zunächst werden Wirtschaftssubjekte betrachtet, die Teilnehmer an einem gemeinsamen Netz oder Dienst sind und damit auch denselben Informationssicherheitsstandard haben. Anschließend wird der Fall untersucht, wo es sich um Angehörige unterschiedlicher Kommunikationssysteme handelt, die miteinander kompatibel sind.[514]

Betrachtet man den ersten Fall eines gemeinsamen Kommunikationssystems und unterstellt wie in Kapitel 2.5, daß nur netz- und dienstweite und keine teilnehmeranschlußbezogenen Informationssicherheitsmaßnahmen möglich sind, dann sind negative Externalitäten zwischen den Teilnehmern nicht zu erwarten. Denn aufgrund des einheitlichen Informationssicherheitstandards ist es für keinen der Teilnehmer möglich, das Sicherheitsniveau der anderen negativ zu beeinflussen. Läßt man dagegen die Möglichkeit zu, daß im Endgerätebereich teilnehmerspezifisch

---

512 Genaugenommen können Informationsasymmetrien auch als Ursache für externe Effekte verstanden werden, weil sie zu einem monetär nicht kompensierten Auseinanderfallen von Leistung und Gegenleistung führen können. Vgl. Meyer (1990), S. 105.

513 Vgl. dazu Übersicht 10 auf S. 203.

514 In der Notation von Kapitel 2.4 handelt es sich im ersten Fall darum, daß Teilnehmer aus einem Netz (n^*, I^*) eine Kommunikationsbeziehung unterhalten, während im zweiten Sachverhalt nach Abbildung 13 auf S. 154 z. B. ein Teilnehmer aus dem Netz B (n_1^*, I_1^*) mit einem aus dem System C (n_2^*, I_2^*) kommuniziert.

unterschiedliche Sicherheitsmaßnahmen realisiert werden, die einen Einfluß auf die Informationssicherheit der Verbindungen mit anderen Anschlüssen haben, dann können Teilnehmer mit unterdurchschnittlichen Informationssicherheitsvorkehrungen in ihrem Endgerätebereich negative externe Effekte für die übrigen mit ihnen kommunizierenden Einheiten verursachen.[515]

Dieselbe Konstellation stellt sich auch dann ein, wenn Teilnehmer aus Kommunikationssystemen mit unterschiedlichem Informationssicherheitsstandard kommunizieren. Denn es wird ebenfalls die Informationssicherheit derjenigen mit einem qualitativ hochwertigen Sicherheitssystem ihres Netzes oder Dienstes negativ von Teilnehmern eines Netzes mit geringem Schutzlevel beeinflußt. Externalitäten bezüglich der Informationssicherheit treten also immer bei Kommunikationsverbindungen zwischen Teilnehmern aus Netzen mit unterschiedlichen Informationssicherheitsstandards oder mit verschiedenem Sicherheitsniveaus im teilnehmerinternen Bereich auf, wobei lediglich die Systeme der Teilnehmer mit geringerem Informationssicherheitsschutz negative Effekte für die Teilnehmer an sichereren Systemen bzw. Endeinrichtungen auslösen. Dagegen erzeugen umgekehrt letztere ersteren nur bedingt positive Externalitäten, weil vor allem absichtliche Angriffe auf das schwächste Glied einer Kommunikationsverbindung abzielen werden und damit die gut gesicherten Komponenten einer Kommunikationsverbindung einen nur begrenzten positiven Effekt auf die Gesamtsicherheit erzeugen.

Nachdem die Existenz von negativen Externalitäten zwischen Kommunikationsteilnehmern identifiziert wurde, stellt sich nun die Frage, inwieweit der Marktprozeß unfähig ist, diese zu internalisieren, und dadurch Allokationsineffizienzen ausgelöst werden, die einen staatlichen Eingriff bedingen.

Betrachtet man die Situation innerhalb eines Kommunikationsnetzes, dann zeichnen sich die Teilnehmer durch ähnliche Kommunikationspräferenzen aus, so daß auch ein gleichgerichtetes Interesse hinsichtlich der Informationssicherheit ihrer Kommunikationsbeziehungen unterstellt werden kann.[516] Außerdem kann bei der Übertragung wichtiger bzw. folgenreicher Informationen davon ausgegangen wer-

---

515 Ein Indiz dafür ist die Diskrepanz zwischen den umfangreichen Informationssicherheitsmaßnahmen bei der zentralen Datenverarbeitung und den gering verbreiteten Schutzmechanismen im Endgerätebereich und bei der Telekommunikation, welche die KES-Sicherheitsstudie 1994 von Gartner & Konrad (1994), S. 10 offenbart.

516 Außerdem haben für gewöhnlich beide Kommunikationsteilnehmer, analog zum Güterverkehr Lieferanten und Empfänger, ähnliche Interessen hinsichtlich der Sicherheit des gemeinsamen Kommunikationsvorgangs, weil durch Verletzungen der Informationssicherheit die Wohlfahrt beider negativ beeinträchtigt wird.

den, daß die Kommunikationspartner in einer vertraglichen Geschäftsverbindung zueinander stehen. Diese Gründe sprechen dafür, daß Sender und Empfänger in der längerfristigen Betrachtung keinen Anreiz haben, durch nachlässiges Verhalten im Endgerätebereich die Informationssicherheit des gemeinsamen Kommunikationsprozesses zu gefährden, und damit in vielen Fällen keine negativen Externalitäten auftreten werden.[517] Dieses Verhalten kann durch den Grundgedanken der kooperativen Verhandlungslösung von Coase[518] erklärt werden, in welcher der Geschädigte den Schädiger für eine Reduktion seiner negative Externalitäten verursachenden Aktivität kompensiert. In diesem Kontext und in Abbildung 20 bedeutet dies, daß derjenige mit einem höheren Informationssicherheitsniveau demjenigen mit einem weniger sicheren Informationssicherheitssystem im Endgerätebereich eine finanzielle Entschädigung für dessen Nettokosten[519] der Harmonisierungsbestrebungen hinsichtlich der gemeinsamen Informationssicherheit bis maximal zur Bruttokompensation anbietet.[520] Diese Vereinbarung stellt letztlich beide um die Fläche der Nettokompensation besser, wobei eine Aufteilung entsprechend der individuellen Verhandlungsposition erfolgt. Das Ergebnis des Verhandlungsprozesses ist der optimale Harmonisierungsgrad, der im Beispiel von Abbildung 20 geringer als die vollständige Harmonisierung der Informationssicherheit ausfällt.[521]

Für Teilnehmer unterschiedlicher Kommunikationssysteme kann argumentiert werden, daß diese i. d. R. Kommunikationsbeziehungen mit einem geringeren Informationssicherheitsbedürfnis unterhalten und damit die zwischen ihnen anfallenden Externalitäten von ihrer Bedeutung nachrangig sind. Im Rahmen von Abbildung 20 bedeutet dies, daß die Grenznutzenkurve aus der Harmonisierung der Informationssicherheit nahezu mit der Abszisse zusammenfällt und damit der optimale Harmonisierungsgrad gleich null ist.[522]

---

517 Beabsichtigte oder zufällige Verletzungen der Informationssicherheit der gemeinsamen Kommunikationsverbindung können durch das Vertrags- und Haftungsrecht sanktioniert werden. Vgl. dazu Abschnitt 2.7.3.

518 Vgl. dazu Coase (1960).

519 Die Nettogrenzkosten der Harmonisierung für den Teilnehmer mit geringerer Informationssicherheit stellen die Differenz zwischen den anfallenden Bruttogrenzkosten und dem ihm selbst zufallenden Grenznutzen aus der Verbesserung seines Informationssicherheitsniveaus dar.

520 Durch private vertragliche Vereinbarungen zwischen den beiden Kommunikationspartnern kann auch das Verursacher-Prinzip durchgesetzt werden, wobei nach der Effizienzthese derselbe Harmonisierungsgrad realisiert wird.

521 Es sind durchaus Grenznutzen-Grenzkosten-Kombinationen denkbar, wo der optimale Harmonisierungsgrad mit der vollständigen Harmonisierung zusammenfällt.

522 Die Sicherheitsniveaus verschiedener Kommunikationssysteme können jedoch durch Informationssicherheitssysteme im Anschlußbereich der jeweiligen Teilnehmer nahezu harmonisiert werden.

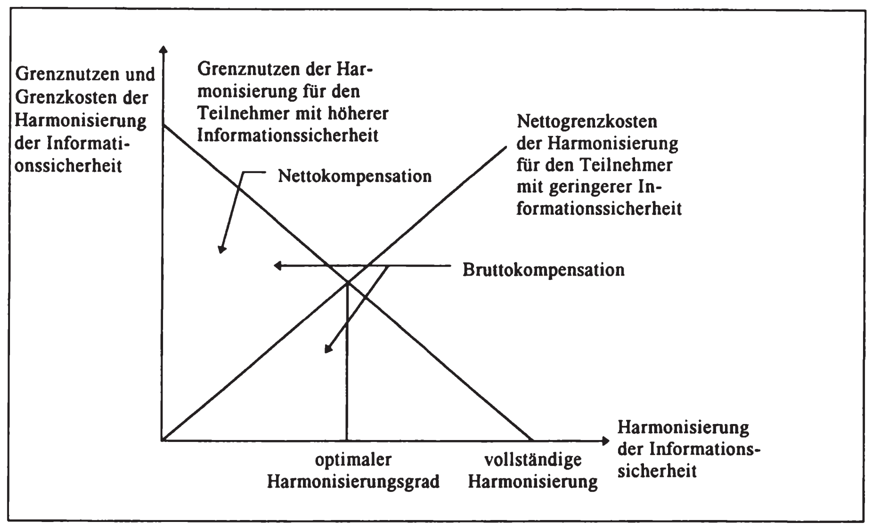


Abb. 20: Die private Verhandlungslösung zur Harmonisierung unterschiedlicher Informationssicherheitsniveaus

Faßt man die Ergebnisse der vorangegangenen Untersuchung zusammen, dann muß zwar festgestellt werden, daß zwischen Kommunikationsteilnehmern negative Externalitäten hinsichtlich der Informationssicherheit auftreten können. Aber entweder sind diese externen Effekte so bedeutend, daß bei den betroffenen Wirtschaftssubjekten massive Anreize bestehen, sie durch private Vereinbarungen freiwillig zu internalisieren, oder sie sind von geringerer Bedeutung, so daß die daraus folgenden Allokationsineffizienzen auch keinen staatlichen Eingriff legitimieren können. Jedoch können die bei den Verhandlungen anfallenden Transaktionskosten u. U. prohibitiv hoch und die Informationen über Grenzkosten und -nutzen zwischen den Verhandlungspartnern asymmetrisch verteilt sein.[523] Dann sollte der Staat durch eine entsprechende Ausgestaltung des Haftungsrechts das dargestellte victim-pays-principle durch das Verursacherprinzip ersetzen, damit eine Verbesserung der Allokation erreicht werden kann.[524]

Dazu können die verschiedenen Systeme der Abteilung Telesec der Deutschen Telekom AG beitragen.

523 Vgl. zu Ineffizienzen der Verhandlungslösung bei Berücksichtigung von Transaktionskosten und asymmetrischer Informationsverteilung Bauer & Illing (1992) und Buchholz & Haslbeck (1991).

524 Die Unzulänglichkeiten des Haftungsrechts verlangen u. U. weitergehende staatliche Eingriffe. Vgl. dazu allgemein Abschnitt 1.5.3 und speziell zur Haftung bei Verletzungen der Informationssicherheit Abschnitt 2.7.3.

2.6.3.2 Externalitäten zwischen Kommunikationsteilnehmern und indirekt betroffenen Nicht-Teilnehmern

Neben den internen Beziehungen zwischen den Kommunikationsteilnehmern gilt es schließlich noch zu untersuchen, inwieweit Verletzungen der Informationssicherheit innerhalb der Kommunikationsnetze und -dienste Externalitäten für nicht unmittelbar betroffene Wirtschaftssubjekte hervorrufen.

Grundsätzlich sind zwar auch die positiven Externalitäten der Informationssicherheitssysteme von Kommunikationsnetzen und -diensten für die übrigen Gesellschaftsmitglieder zu berücksichtigen. Aber diese Sicherheitsmaßnahmen liegen im besonderen Interesse der Teilnehmer, so daß sie zumindest bis zum Ausgleich von teilnehmerspezifischen Grenzkosten und -nutzen realisiert werden. Ferner ist vor allem in den Vereinigten Staaten ein heftiger Konflikt zwischen der nationalen Sicherheitsbehörde NSA (=National Security Agency), die sich um die innere und äußere Sicherheit bemüht, und Gruppen, die die informationelle Selbstbestimmung der Bürger schützen wollen, darüber entbrannt, wie die Informationssicherheit in Kommunikationsnetzen mittels moderner Chiffrierverfahren realisiert werden soll.[525] Die erste Gruppe befürchtet durch die Verwendung der sogenannten asymmetrischen Kryptosysteme eine Gefährdung innerer und äußerer Sicherheit, weil diese Strafverfolgungs- und Geheimdienstaktivitäten der staatlichen Behörden behindern oder gar unterbinden können. Dagegen befürwortet die Gemeinde der Daten- und Privacyschützer deren Implementierung, denn damit ist die Informationssicherheit der Bürger ohne staatlich organisierte Schlüsselverwaltung, die u. a. die Abhörung durch staatliche Sicherheitsbehörden erlaubt, möglich. Diese Diskussion zeigt, daß nicht eindeutig bestimmt werden kann, ob die Informationssicherheitssysteme von Kommunikationsnetzen für die Gesellschaft positive oder negative Externalitäten erzeugen, so daß sich bei der folgenden Untersuchung auf die negativen Externalitäten der Verletzungen der Informationssicherheit beschränkt wird.[526]

---

525 Vgl. dazu Rihaczek (1993), Rueppel (1994) und Levy (1994). Während in den USA bereits mit kryptotechnischen Aspekten argumentiert wird, ist die Diskussion in der Bundesrepublik um den „Lauschangriff“ zunächst von rechtlichen, aber inzwischen auch von Kostengesichtspunkten geprägt, da sich die D-Netzbetreiber weigern, die Aufwendungen für die Abhörungseinrichtungen zu bezahlen. Vgl. o. V. (1995a), (1995b).

526 Die Abwägung zwischen verschiedenen Rechtsgütern bedarf letztlich einer politischen Entscheidung. Inzwischen existieren auch organisatorische und technische Vorschläge, die einen Kompromiß zwischen beiden Anforderungen ermöglichen. Vgl. Leiberich (1995).

Während Schäden an der Hard- oder Software der Kommunikationssysteme vor allem die jeweiligen Teilnehmer oder Betreiber von Netzen und Diensten negativ beeinträchtigen, können Verletzungen der Informationssicherheit gerade auch Nicht-Teilnehmer negativ beeinträchtigen.

Hierbei bietet sich bei der Untersuchung der negativen Externalitäten eine Differenzierung der Beeinträchtigung der Informationssicherheit an. Betrachtet man zunächst das Sicherheitskriterium der Verfügbarkeit der transportierten Informationsinhalte, dann werden bei dessen Nichtgewährleistung unmittelbar lediglich die Interessen der kommunizierenden Parteien negativ beeinträchtigt, ohne daß Dritte tangiert werden. Die durch den gleichzeitigen Ausfall mehrerer Vermittlungsstellen verursachten weiterreichenden Folgewirkungen können hingegen die Versorgung der gesamten Bevölkerung mit elementaren Güter- und Dienstleistungen bedrohen.[527]

Während das Nichtzustandekommen von Kommunikationsbeziehungen u. U. Katastrophen nach sich ziehen und damit Teilnehmer und Nicht-Teilnehmer in gleichem Maße treffen kann, werden bei Integritäts- und Vertraulichkeitsverletzungen nur bestimmte Personengruppen betroffen. Werden Kommunikationsinhalte absichtlich oder unabsichtlich verändert, dann haben i. d. R nur die beteiligten Kommunikationspartner die daraus entstehenden Schäden zu tragen. Handelt es sich aber um Informationen, die Nicht-Teilnehmer anbelangen, dann widerfahren auch diesen Schäden aus Verletzungen der Integrität, so daß diese Beeinträchtigungen der Informationssicherheit ebenso negative Externalitäten für bestimmte Personenkreise auslösen.

Ferner ist auf Vertraulichkeitsverletzungen einzugehen. Zwar trifft ein Verstoß gegen die Vertraulichkeit von Kommunikationsinhalten zunächst die kommunizierenden Parteien, jedoch werden analog zu Integritätsbeeinträchtigungen auch Nicht-Teilnehmer negativ tangiert, wenn sich die transportierten Informationen auf ihre Person oder ihr Unternehmen beziehen. Dabei kann u. U. die Konstellation eintreten, daß die Bedeutung dieser Eigenschaft der Informationssicherheit für letztere

---

527 Vgl. dazu Hammer (1991), S. 134f.

höher ist als für die eigentlichen Teilnehmer der Kommunikationsnetze und -dienste und damit bedeutende negative Externalitäten zu erwarten sind.[528]

Schließlich ist noch die Externalitätenproblematik bei Authentifikationsmanipulationen zu diagnostizieren. Die Authentizität von Kommunikationsteilnehmern ist vor allem ein internes Problem der Kommunikationssysteme, so daß Authentizitätsverletzungen vor allem die Teilnehmer von Netzen und Diensten schädigen. Nicht-Teilnehmer werden nur in Einzelfällen in materieller Hinsicht beeinträchtigt, wenn z. B. unautorisierte Abhebungen von Bankkonten vorgenommen werden.

Eigenschaften der Externalitäten / Eigenschaften der Informationssicherheit	Potentiell betroffene Nicht-Teilnehmer	Quantitatives Ausmaß	Qualitativer Charakter[529]
Verfügbarkeit	gesamte Bevölkerung	hoch	materielle Schäden
Integrität	Teilgruppen	mittel	materielle Schäden
Vertraulichkeit	Teilgruppen	mittel	materielle und immaterielle Schäden
Authentizität	Einzelfälle	mittel	materielle Schäden

Übersicht 11: Negative Externalitäten verschiedener Verletzungen der Informationssicherheit

Übersicht 11 faßt die Ergebnisse der Analyse der Externalitäten von Verletzungen der Informationssicherheit in Kommunikationsnetzen und -diensten für die Nicht-Teilnehmer zusammen. Sowohl mit höheren Teilnehmerzahlen n* als auch mit der Leistungsfähigkeit bzw. dem Integrationsgrad I* steigt tendenziell das quantitative Ausmaß aller übrigen negativen externen Effekte von Verletzungen der Informati-

[528] Ein Beispiel dafür ist die Übermittlung von Gesundheitsdaten von Patienten zwischen verschiedenen Akteuren im Gesundheitswesen, wie Ärzten und Krankenhäuser oder -kassen. Vgl. zur Bedeutung der „Telemedizin Adamik" (1995).

[529] Verletzungen der Informationssicherheit ziehen zwar in den meisten Fällen sowohl materielle als auch immaterielle Schäden nach sich, so daß in dieser Spalte lediglich eine Gewichtung der jeweiligen Schadenskategorien versucht wird.

onssicherheit. Letzteres liegt darin begründet, daß das Ausmaß der transportierbaren Informationsmengen mit I* unmittelbar zunimmt. Mit der Expansion verschiedener Kommunikationssysteme wird auch die Anzahl der Nicht-Teilnehmer zunehmen, deren Wohlfahrt durch die negativen externen Effekte von Verletzungen der Informationssicherheit indirekt beeinträchtigt wird.[530]

2.6.3.3 Allokationsineffizienzen aufgrund von Externalitäten

Während die internen Externalitäten zwischen den Kommunikationsteilnehmern durch private Verhandlungen in vielen Fällen internalisiert werden, hat der vorangegangene Abschnitt verdeutlicht, daß die Risiken der Verletzung der Informationssicherheit in Kommunikationsnetzen negative Externalitäten für die übrige Gesellschaft verursachen.[531] Der Wert eines sicheren Kommunikationsvorgangs kommt also nicht nur den Kommunikationsteilnehmern zu, sondern auch Dritten, welche ihre Präferenzen nicht unmittelbar in das Entscheidungskalkül der Netz- und Dienstebetreiber und -teilnehmer über die Informationssicherheit einbringen können.[532] Dies bedeutet, daß die Grenznutzen der Nicht-Teilnehmer in Form der Verminderung ihres Schadenpotentials im Grenznutzen-Grenzkosten-Kalkül der Teilnehmer bezüglich der Installation von Informationssicherheitsmaßnahmen nicht berücksichtigt werden und die daraus folgende Allokationsineffizienz sich in einem zu geringen Niveau an Informationssicherheit in Kommunikationsnetzen und -diensten (r^*_{privat}) ausdrückt. Abbildung 21 macht graphisch die zu erwartenden Wohlfahrtsverluste in Form der grau schraffierten Fläche deutlich.

Abbildung 21 macht ferner anschaulich, daß das externe Schadenpotential bzw. der Grenznutzen von Self-protection-Maßnahmen für Nicht-Teilnehmer mit n* und I* ansteigt, so daß mit diesen Parametern auch die Allokationsineffizienzen zunehmen werden.

---

530 Die absolute Zahl derjenigen Individuen, die an kein Kommunikationssystem angeschlossen sind, nimmt ab. Jedoch werden neu entstehende Kommunikationssysteme zusätzliche Externalitäten verursachen.

531 Vgl. dazu die empirischen Indizien in Fußnote 515.

532 Da, wie in Abschnitt 2.5.3 gezeigt, die Informationssicherheitsmechanismen mehrere Eigenschaften der Informationssicherheit erfüllen können, muß die Differenzierung der Externalitäten nach Übersicht 11 bei der Bestimmung der Allokationsineffizienzen aufgegeben werden.

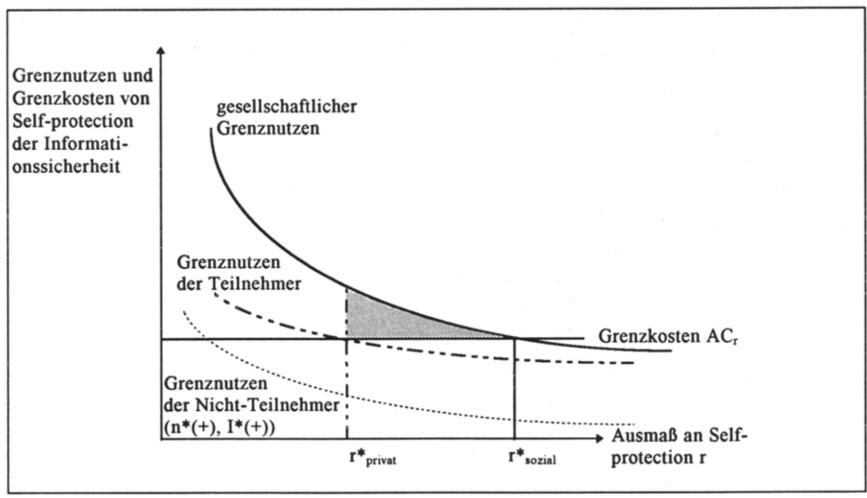


Abb. 21: Externalitäten der Informationssicherheit

2.6.4 Fazit

In diesem Abschnitt sollen die Ergebnisse der vorangegangenen Untersuchung der verschiedenen Ursachen von Allokationsineffizienzen hinsichtlich der Informationssicherheit in Kommunikationsnetzen und -diensten kurz zusammengefaßt und in eine Abbildung integriert werden.

Bezüglich der asymmetrischen Informationsverteilung ist deutlich geworden, daß trotz der privaten Initiativen der Angebots- und der Nachfrageseite Informationsasymmetrien bestehen bleiben und dadurch Wohlfahrtsverluste hervorgerufen werden, die, wie noch zu zeigen ist, mit staatlichen Instrumenten der Wirtschaftspolitik reduziert werden können.

Obwohl die Externalitäten zwischen Kommunikationsteilnehmern durch private Verhandlungslösungen weitgehend internalisiert werden können, bleibt für die negativen externen Effekte (EXT) von Verletzungen der Informationssicherheit innerhalb von Kommunikationssystemen für die Nicht-Teilnehmer bzw. für den Rest der Gesellschaft auch ein staatlicher Handlungsbedarf bestehen. Abbildung 22 zeigt die Diskrepanz zwischen dem realisierten (r_{privat}) und dem gesellschaftlich

optimalen (r^*_{sozial}) Niveau an Informationssicherheitsaufwendungen und den damit verbundenen volkswirtschaftlichen Wohlfahrtsverlust als grau schraffierte Fläche.

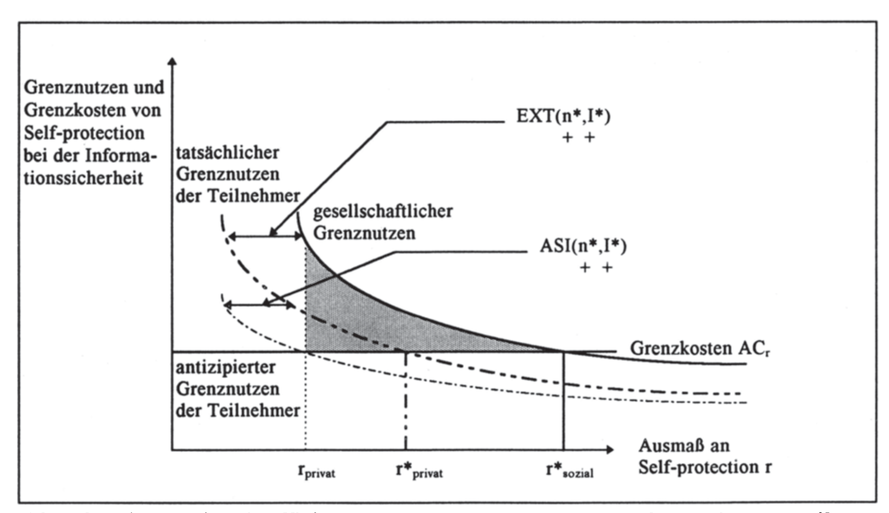


Abb. 22: Allokationsineffizienzen durch asymmetrische Informationsverteilung und negative Externalitäten

Im folgenden Kapitel 2.7 werden staatliche Instrumente danach untersucht, inwieweit sie die asymmetrische Informationsverteilung zwischen Netz- und Diensteanbieter und Kommunikationsteilnehmer und die negativen Externalitäten von Verletzungen der Informationssicherheit auf die übrige Gesellschaft abzubauen vermögen.

2.7 Staatliche Instrumente zur Behebung der Allokationsineffizienzen von Informationssicherheit in Kommunikationssystemen

2.7.1 Vorbemerkungen

Nachdem in Kapitel 2.6 die wesentlichen Ursachen - Informationsasymmetrien und Externalitäten - für die Allokationsineffizienzen in bezug auf die Informationssicherheit in Kommunikationssystemen identifiziert wurden, werden nun die staatlichen Instrumente von Kapitel 1.5 dahingehend untersucht, ob sie in diesem Kontext geeignet sind, Verbesserungen des Informationssicherheitsniveaus verteilungsgerecht und kostengünstig zu erreichen. Die Untersuchung basiert zwar auf normativen allokationstheoretischen Überlegungen, aber sie nimmt einen direkten Bezug zu den institutionellen Gegebenheiten in der Bundesrepublik Deutschland.

Die folgende Übersicht[533] 12 gibt einen Überblick über die möglichen Ansatzpunkte der verschiedenen Instrumente der Wirtschaftspolitik.[534] Im nachfolgenden Abschnitt werden zuerst die Informationspolitik, danach die Haftung der Netz- und Dienstebetreiber, anschließend verschiedene Subventionslösungen, darauf die Regulierung mittels Mindestsicherheitstandards und zuletzt die direkte staatliche Förderung von Forschungs- und Standardisierungsaktivitäten im Bereich der Informationssicherheit in Kommunikationsnetzen und -diensten dargestellt und begutachtet. In der abschließenden Bewertung werden die staatlichen Instrumente, die zum Abbau der Informationsasymmetrien und der negativen Externalitäten geeignet sind, in Beziehung zueinander gestellt.

Es sind zwar auch strafrechtliche Maßnahmen[535] möglich, indem Computerkriminalität intensiver verfolgt und härter bestraft wird, jedoch ist die Wirksamkeit relativ gering[536], so daß auf deren Darstellung verzichtet und sich auf die wirtschaftspolitischen Instrumente zur Verbesserung der Informationssicherheitssysteme in Kommunikationssystemen konzentriert wird.

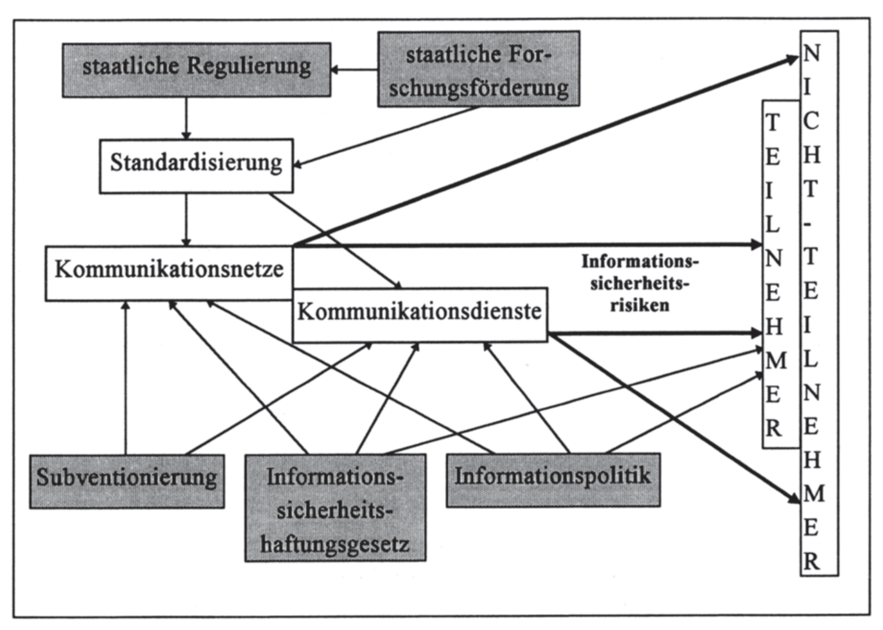
---

533 In Anlehnung an Kubicek (1991), S. 57.

534 Vgl. zur Auflistung möglicher staatlicher Instrumente auch Ulrich (1995).

535 Vgl. zur rechtlichen Risikosteuerung im allgemeinen Roßnagel (1984), S. 198-220.

536 Vgl. dazu auch Katz (1991), S. 63f. So ist fünf Jahre nach Einführung des „Computer Fraud and Abuse Act" - ein umfassendes Gesetz gegen Computermißbrauch und -kriminalität - in den USA lediglich eine Person danach verurteilt worden. Dafür spricht auch die geringe Zahl der angezeigten Fälle und die niedrige Aufklärungsraten bei der Computerkriminalität in der BRD. Vgl. zu den aktuellen Deliktsformen und zur Reaktion der Gesetzgeber Sieber (1995).



Übersicht 12: Staatliche Instrumente zum Abbau von Allokationsineffizienzen

2.7.2 Die staatliche Informationspolitik

2.7.2.1 Die Ziele der staatlichen Informationspolitik

Wie der Begriff schon andeutet ist die staatliche Informationspolitik im Bereich der Informationssicherheit in Kommunikationsnetzen und -diensten vor allem darauf gerichtet, sowohl den unvollständigen Informationszustand besonders der Teilnehmer als auch die asymmetrische Informationsverteilung zwischen den Nachfragern und der Anbietern abzubauen, so daß die daraus resultierenden gesellschaftlichen Wohlfahrtsverluste reduziert werden können. Zu einer Internalisierung negativer Externalitäten kann sie nur mittelbar beitragen, indem zum einen die asymmetrische Informationsverteilung zwischen Teilnehmern unterschiedlicher Kommunikationssysteme abgebaut und damit die Ergebnisse der privaten Internalisierungsbe-

mühungen verbessert werden.[537] Zum anderen können die indirekt betroffenen Nicht-Teilnehmer verstärkt über die sie betreffenden Risiken der Informationssicherheit aufgeklärt werden, damit sie ihre Interessen in den damit befassenden politischen Entscheidungsprozessen besser vertreten und durchsetzen können.[538] Dieser Aspekt wird bei den Ausgestaltungsvorschlägen der verschiedenen Instrumente der Informationspolitik nicht weiter berücksichtigt, sondern es wird sich vor allem auf den Abbau der Informationsasymmetrien über die Informationssicherheit zwischen den Anbietern und Nachfragern von Kommunikationsdienstleistungen bezogen.

In einem ersten Schritt wird untersucht, inwieweit durch staatliche Eingriffe die Informationssicherheit betreffenden Signaling-Anstrengungen der Anbieter von Kommunikationsnetzen und -diensten effizient unterstützt werden können. Anschließend werden Möglichkeiten dargestellt, wie die Screening-Bemühungen der Nutzer von Kommunikationsdienstleistungen hinsichtlich ihrer Informationssicherheit mittels staatlicher Unterstützung an Effizienz gewinnen können.

2.7.2.2 Informationsvorschriften für die Betreiber von Kommunikationsnetzen und -diensten

Obwohl durchaus auf Seiten der Betreiber von Kommunikationsnetzen und -diensten Anreize existieren, die Qualität ihrer Produkte und Dienstleistungen hinsichtlich Informationssicherheit den Nachfragern zu signalisieren, hat die Analyse in Abschnitt 2.6.2.3 ergeben, daß diese nicht ausreichen, um die Informationsasymmetrien auf ein aus Effizienzgesichtspunkten zufriedenstellendes Maß zu reduzieren.[539] Da die Angebotsseite am kostengünstigsten Informationen über die Schadenswahrscheinlichkeiten und -potentiale und über die Effektivität der Informationssicherheitssysteme ihrer Kommunikationssysteme beschaffen kann, sollten

[537] Werden die Grenznutzen- und Grenzkostenverläufe aus Abbildung 20 auf S. 216 von den Verhandlungspartnern falsch antizipiert, dann kommt es zu keiner allokationseffizienten Harmonisierung der Informationssicherheit. Vgl. allgemein dazu Buchholz & Haslbeck (1991), S. 171ff.

[538] So schlagen das System Security Study Committee u. a. (1991), S. 162, für die Vereinigten Staaten ein langfristiges Erziehungsprogramm vor, das schon frühzeitig auf die Gefahren von Computer- und Kommunikationssystemen aufmerksam macht.

[539] Die negativen Externalitäten, denen Nicht-Teilnehmer durch Verletzungen der Informationssicherheit im Rahmen der Datenverarbeitung bzw. der Nutzung von Kommunikationssystemen öffentlicher und nicht-öffentlicher Stellen ausgesetzt sind, sollen in der Bundesrepublik Deutschland durch die Bestimmungen des BDSG begrenzt werden.

sie im Rahmen des neu zu verfassenden Telekommunikationsgesetzes[540] einer ausdrücklichen Informationspflicht unterliegen, wobei den Nachfragern Informationen über sämtliche Risikopotentiale in einer verständlichen Art und Weise nahegebracht werden sollten.[541]

Obwohl sich diese Lösung durch die kostengünstige Informationsgewinnung und -verbreitung durch die Anbieter auszeichnet und vor allem Privatpersonen zugute kommt, für die die Kosten der Informationsbeschaffung u. U. prohibitiv hoch sind, hat sie Schwächen. Zum einen liegen auch den Anbietern besonders im Bereich beabsichtigter Angriffs- und Manipulationsversuche und bei Vertraulichkeitsverletzungen nur unvollständige Informationen über die aktuellen Risiken und die Effektivität der Informationssicherheitssysteme vor. Zum anderen sind die Sanktionsmöglichkeiten bei der Verbreitung von Falschinformationen über den Stand der Informationssicherheit begrenzt, weil die Kontrollbehörden diese nur in wenigen Fällen mittels objektiven Beweisen widerlegen können.[542]

In einem nächsten Schritt gilt es deshalb zu untersuchen, inwieweit die Informationsgewinnungsbemühungen der Nachfrager effizient unterstützt werden können.

2.7.2.3 Staatliche Subventionierung der Gewinnung und Verbreitung von Informationen über die Informationssicherheit von Kommunikationsnetzen und -diensten

Aufgrund der Öffentlichen-Guts-Eigenschaften von Informationen ist auch das private Angebot an allgemeinen Informationen über die Informationssicherheit von Kommunikationssystemen unzureichend bzw. nicht existent.[543] Deshalb ist es gesamtwirtschaftlich gesehen wohlfahrtssteigernd, wenn der Staat vor allem die Informationen, welche die Eigenschaften reiner öffentlicher Güter haben, sowohl produziert als auch kostenlos oder verbilligt an die Teilnehmer und die indirekt betroffenen Nicht-Teilnehmer verbreitet.

---

[540] Vgl. das Bundesministerium für Post und Telekommunikation (1995) und zur aktuellen Fassung der Telekommunikationsverordnung (TKV) BGBl. S. 1717 vom 13. 10. 1992.

[541] Vgl. zur gesetzlichen Kennzeichnungspflicht im Rahmen der Verbraucherpolitik Kuhlmann (1990), S. 161ff.

[542] Außerdem gibt es innerhalb der Gruppe der Informationssicherheitsexperten immer noch eine heftige Diskussion um die adäquate Bestimmung der notwendigen Eigenschaften der Informationssicherheit. Vgl. dazu Rannenberg (1994).

[543] Das Beratungsangebot über informationstechnische Sicherheitsaspekte richtet sich vor allem an professionelle Datenverarbeiter und stellt kein öffentliches, sondern ein privates Gut dar, so daß eine staatliche Intervention aus Allokationsgründen nicht gerechtfertigt werden kann.

Hinsichtlich der Informationssicherheit in Kommunikationsnetzen können zwei Klassen von Informationen unterschieden werden. Zum einen erleichtert die zentrale Erfassung und Dokumentierung von Schadensfällen[544] in Kommunikationsnetzen und -diensten den Nachfrager analog zur Unfallstatistik des Straßenverkehrs die Einschätzung der Qualität der Informationssicherheit des vielfältigen Angebotes an Kommunikationssystemen.[545] Außerdem wird infolgedessen indirekt bei den Betroffenen das Bewußtsein über das Schadenpotential verbessert. Insgesamt kann dadurch die asymmetrische Informationsversorgung der Teilnehmer hinsichtlich des erwarteten Schadens, der durch die Nutzung von Kommunikationsnetzen und -diensten verursacht wird, abgebaut werden. Zum anderen sollten informationstechnische Systeme in bezug auf die Kriterien der Informationssicherheit von einer staatlichen zugelassenen Institution, die ein gewisses Maß an allgemeinem Vertrauen und breiter Akzeptanz genießt, geprüft und diese Ergebnisse allen potentiellen Teilnehmern von Kommunikationssystemen und sonstigen Interessierten zugänglich gemacht werden.[546]

In der Bundesrepublik Deutschland existiert seit 1991 das Bundesamt für Sicherheit in der Informationstechnik BSI, das u. a. im Rahmen der staatlichen Informationspolitik mit der Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen und Komponenten und der Erteilung von Sicherheitszertifikaten[547] und der Beratung von Herstellern, Vertreibern und Anwendern über die Thematik der Informationssicherheit betraut ist.[548] Diese Institution erfüllt also bereits wesentliche Teile der Aufgaben der vorgeschlagenen staatlichen Informationsversorgung im Bereich der Informationssicherheit. Sie sollte jedoch durch die angesprochene zentrale Schadensdokumentationsstelle erweitert werden. Ferner ist eine aktive Ausdehnung ihrer Beratungstätigkeit auf Privatpersonen angebracht[549], denn der Bekanntheitsgrad des BSI ist selbst unter professionellen Datenverarbeitern

---

544 Vgl. dazu auch das System Security Study Committee u. a. (1991), S. 163.

545 Hierzu müssen die Betreiber von Netzen und Diensten zu einer ausführlichen Berichterstattung von Schadensfällen gesetzlich verpflichtet werden, da sie selbst aufgrund drohender Nachfragerückgänge an keiner Veröffentlichung interessiert sind.

546 Diese sogenannte Zertifizierung von informationstechnischen Systemen kann nicht nur als Erleichterung der Screening-Bemühungen angesehen werden, sondern ist auch im Interesse der Anbieter von qualitativ hochwertigen Produkten, weil durch die Bestätigung einer objektiven Prüfstelle die Glaubwürdigkeit ihrer Signaling-Anstrengungen gestärkt wird.

547 Das BSI hat auch die Kompetenz, weitere Prüfstellen, wie verschiedene private Beratungsunternehemen oder technische Überwachungsvereine, zuzulassen. Vgl. dazu BSI (1993), S. 6f.

548 Vgl. zu den Aufgaben des BSI das BGBl. S. 2834 vom 17. 12. 1990.

549 So kritisieren auch Pfitzmann & Rannenberg (1993), S. 179, daß sich die Aktivitäten des BSI vor allem auf die Belange der Betreiber und nur begrenzt auf die der Nutzer von Informationstechnik konzentrieren und die Datenschutzinteressen der Bürger völlig vernachlässigt werden.

begrenzt.[550] Schließlich erfolgt eine Zertifizierung von informationstechnischen Produkten nur auf Antrag bzw. mit Zustimmung der Hersteller. Hier müßte die Kompetenz des BSI insoweit ausgedehnt werden, daß ihm die Prüfung kompletter Kommunikationssysteme nach objektiven Kriterien auf eigene Initiative hin erlaubt wird.

2.7.2.4 Die Bewertung des informationspolitischen Instrumentariums

Nach der Darstellung der staatlichen Instrumente der Informationspolitik gilt es nun eine Bewertung nach allokativen, distributiven und fiskalischen Kriterien vorzunehmen.

Im allgemeinen richtet sich die staatlichen Informationspolitik ausschließlich auf die asymmetrischen Informationsverteilungen. Für eine Internalisierung der externen Effekte aufgrund fehlender Anreize bzw. Sanktionen ist sie ungeeignet. Differenziert man die Informationspolitik nach ihren Ansatzpunkten, dann ist die Effektivität von Informationsvorschriften für die Anbieter von Netzen und Diensten begrenzt, weil die Überprüfungsmöglichkeiten der Angaben und damit auch die Sanktionsmöglichkeiten beschränkt sind. Aus Allokationsgesichtspunkten erfolgversprechender sind die staatlich subventionierten Aktivitäten zur Informationsgewinnung und die kostenlose Verbreitung von Kenntnissen über die Informationssicherheit von Kommunikationsnetzen und -diensten, die die asymmetrische Informationsverteilung vor allem durch die Verbesserung des Informationsstandes der Nachfrager abbauen sollen.

Betrachtet man die Verteilungseffekte von Informationsvorschriften für den Anbieter von Kommunikationsnetzen und -diensten, so muß konstatiert werden, daß die dadurch entstehenden Kosten letztendlich durch die Überwälzung auf den Preis von den Nachfragern getragen werden, die auch die eigentlichen Nutznießer solcher Kennzeichnungspflichten sind. Im Gegensatz dazu muß die gesamte Gesellschaft, also auch die Gruppe der nicht betroffenen Nicht-Teilnehmer, für die Kosten staatlicher Zertifizierungs- und Beratungsstellen aufkommen, obwohl die Begünstigten lediglich die Anbieter von zertifizierten Produkten und die potentiellen Anwender von Kommunikationssystemen mit Informationssicherheitsrisiken sind,

[550] So waren die Zertifizierungsaktivitäten nur der Hälfte und die Beratungstätigkeiten des BSI nur einem Drittel der Befragten der KES-Sicherheitsstudie 1994 bekannt. Vgl. dazu Gartner & Konrad (1994), S. 13f.

so daß eine gewisse Eigenbeteiligung angebracht ist. Trotzdem sollten diese Aufgaben mit staatlichen Mitteln subventioniert werden, gerade wenn es sich um Informationen handelt, die die Eigenschaften eines reinen öffentlichen Gutes erfüllen. Des weiteren können die infolge des Abbaus von Informationsasymmetrien erfolgten Verbesserungen der Informationssicherheit in Kommunikationssystemen u. U. positive Externalitäten für nur mittelbar betroffene Nicht-Teilnehmer auslösen, was zumindest eine Teilsubventionierung der Informationsbereitstellung rechtfertigt.

Hinsichtlich der Gesamthöhe der fiskalischen Kosten ist zwar das Erlassen von Informationsvorschriften kostengünstiger, jedoch kann die Unterhaltung einer staatlichen Institution wie dem BSI angesichts der von ihr verursachten positiven Wohlfahrtseffekte und der geringen negativen Nebenwirkungen als gerechtfertigt angesehen werden.[551]

2.7.3 Die Haftung der Betreiber von Kommunikationsnetzen und -diensten für Verletzungen der Informationssicherheit

2.7.3.1 Die Ziele der Haftung der Betreiber von Kommunikationsnetzen und -diensten

Während die staatliche Informationspolitik auf die Risiken für die Informationssicherheit in Kommunikationsnetzen und -diensten keinen direkten und mit Sanktionen ausgestatteten Einfluß auf die Sicherheitsaktivitäten der Anbieter und Nachfrager hat, wirken Haftungsregeln durch die Zuordnung von Verantwortlichkeiten und die Bestimmung von Kompensationsleistungen nach dem Eintritt eines Schadenfalls auch unmittelbar auf die Präventionsaktivitäten.[552] Im Gegensatz zur Informationspolitik, die lediglich darauf zielt, Informationslücken und -asymmetrien abzubauen, können durch eine adäquate Ausgestaltung des Haftungsrechtes sowohl In-

---

[551] Der Gesamthaushalt des BSI hat 1992 63 Millionen DM betragen, wobei damit auch die noch darzustellende Zulassung von Informationssicherheitssystemen und die Forschungsaktivitäten im Bereich der Informationssicherheit finanziert werden. Vgl. o. V. (1992), S. 133. Außerdem kann davon ausgegangen werden, daß in einer Institution, die verschiedene Aufgaben in einem Bereich wahrnimmt, positive Synergieeffekte auftreten. Jedoch kritisieren Pfitzmann & Rannenberg (1993), S. 179, die Vielfachfunktion des BSI, weil keine wesentlichen Fortschritte in der Informationssicherheit besonders für die Datenschutzbelange der Bürger zu verzeichnen seien.

[552] Vgl. dazu genauer Abschnitt 1.5.3.

formationsasymmetrien abgebaut als auch eine Internalisierung der durch die Verletzung der Informationssicherheit ausgelösten externen Effekte erreicht werden.

In diesem Abschnitt sollen die allokativen Effekte von Verschuldens- und Gefährdungshaftung auf das Niveau an Informationssicherheit in Kommunikationssystemen gegenübergestellt werden. Zunächst wird auf die Verringerungen der Informationsasymmetrien durch die Produkthaftung der Betreiber von Kommunikationsnetzen und -diensten und anschließend auf die Internalisierung der negativen externen Effekte durch die Rechtsregelungen im allgemeinen Bereich unerlaubter Handlungen eingegangen.[553] Da die Regelungen des aktuellen Produkthaftungsgesetzes (ProdHaftG)[554] der Bundesrepublik Deutschland nicht auf Kommunikationsdienstleistungen anzuwenden sind[555], werden lediglich die Haftungsbestimmung von §17 der Neufassung der Telekommunikationsverordnung[556] (TKV) und von §7f des BDSG auf ihre allokativen Implikationen für das Informationssicherheitsniveau untersucht. Abschließend werden die Elemente eines auch durch die Liberalisierung des Telekommunikationsmarktes notwendig gewordenen Informationssicherheitshaftungsgesetzes von Netz- und Dienstebetreibern analog zum Umwelthaftungsgesetz (UmweltHG)[557] vorgestellt, das allokative, distributive und administrative Gesichtspunkte berücksichtigt.

2.7.3.2 Verschuldens- versus Gefährdungshaftung der Betreiber von Kommunikationsnetzen und -diensten zur Reduktion von Informationsasymmetrien

Da in Kapitel 2.6 hinsichtlich der Häufigkeit der Verletzung der Informationssicherheit bzw. über die Effizienz der Informationssicherheitssysteme in Kommunikationsnetzen und -diensten ein Informationsdefizit zuungunsten der Nachfrager

---

553 Es wird in realistischer Weise von sogenannten unilateralen Schäden, d. h. wiederum von der alleinigen Möglichkeit der Anbieter zu netz- bzw. dienstbetreffenden Maßnahmen der Informationssicherheit ausgegangen, so daß die Anwender und die indirekt Betroffenen selbst keine Schadensprävention betreiben können.

554 Vgl. dazu BGBl. S. 2198 vom 15. 12. 1989 und eine allgemeine ökonomische Analyse von Finsinger & Simon (1989), S. 185-214.

555 Vgl. dazu Büchner (1992), S. 110f. Überdies werden die Haftungsregelungen in §9 des Gesetzes über die Regulierung der Telekommunikation und des Postwesens (PTRegG), BGBl. S. 2371 vom 22. 9. 1994, für die Deutsche Telekom AG und auch im Eckpunkte-Papier des Bundesministerium für Post und Telekommunikation (1995), S. 14, über den künftigen Regulierungsrahmen nicht weiter konkretisiert.

556 Vgl. BGBl. S. 1717 vom 5. 10. 1992.

557 Vgl. BGBl. S. 2634 vom 14. 12. 1990.

identifiziert wurde, stellt sich nun die Frage, ob die Verschuldenshaftung der Anbieter[558] von Netzen und Diensten zu einer ausreichenden Allokationsverbesserung beitragen kann oder ob die strengere Form der Gefährdungshaftung angebracht ist.

Die ökonomischen Anreize der Verschuldenshaftung sorgen dafür, daß die Angebotsseite den vom Gesetzgeber verordneten Sorgfaltsstandard einhält, bzw. wenn dieser übermäßig streng ist, daß freiwillig das gleiche Niveau wie bei der Gefährdungshaftung realisiert wird. Die Nachfragerseite kann deshalb davon ausgehen, daß das Angebotssegment mit einem geringen Informationssicherheitsstandard ausscheidet, der Umfang asymmetrischer Informationsverteilung dadurch ab- und die durchschnittliche Zahlungsbereitschaft für Informationssicherheitsmaßnahmen zunimmt. Es kann also eine gesamtwirtschaftliche Wohlfahrtssteigerung erwartet werden, die sich durch eine Rechtsverschiebung der antizipierten Grenznutzen in Abbildung 19 auf S. 212 als eine Verkleinerung des schraffierten Dreiecks widerspiegelt.

Die Vorteilhaftigkeit der Verschuldenshaftung wird jedoch durch die folgenden besonderen Aspekte bezüglich der Informationssicherheit in Kommunikationssystemen begrenzt.[559] Zunächst besteht die Gefahr, daß der Gesetzgeber aus Unkenntnis der Schadenpotentiale oder wegen des Widerstandes der Anbieterseite einen zu geringen, unter dem volkswirtschaftlichen Optimum liegenden Sorgfaltsstandard von den Anbietern verlangt.[560] In diesem Fall liegt der Mindeststandard an Informationssicherheit unter dem volkswirtschaftlich optimalen Niveau. Die Informationsasymmetrie zuungunsten der Nachfrager wird nur begrenzt ab- und deren durchschnittliche Zahlungsbereitschaft nicht wesentlich zunehmen. Außerdem muß besonders bei Vertraulichkeitsverletzungen damit gerechnet werden, daß ex post eine gewisse Unsicherheit über den Verletzer der Informationssicherheit besteht und der Anbieter nicht immer zur Schadenskompensation herangezogen wird. Dies führt aber nur dann zu einer Unterschreitung des geforderten Sorgfaltsstandards, wenn dem Anbieter in relativ vielen Fällen keine Schuld nachgewiesen werden

---

558 Die Angebotsseite wird nicht in Netz- und Diensteanbieter differenziert, obwohl Fehlerursachen sowohl im Netz- als auch im Dienstebereich liegen können, weil diese Unterscheidung nur kompliziertere Haftungsbeziehungen ohne zusätzlichen Erkenntnisgewinn mitsichbringen würde.

559 Es wird wiederum von einer homogenen Teilnehmermenge ausgegangen, so daß kein Teilnehmer aufgrund fehlender eigenständiger Möglichkeiten zu Informationssicherung durch diesen netzweiten Sicherheitsstandard, der den Optimalitätsbedingungen von Kapitel 2.5 entspricht, einen individuellen Wohlfahrtsverlust erleiden muß, wie er durchaus bei heterogenen Konsumenten auftreten kann.

560 Vgl. dazu Endres (1991), S. 112ff.

kann.[561] Analog kann im Fall der Risikounterschätzung und der Haftungsbeschränkungen argumentiert werden. Auch hier müssen diese sehr gravierend ausfallen, damit der Anbieter den geforderten Sorgfaltsstandard nicht erfüllt.[562] Die schwierige Monetarisierung immaterieller Schäden, die, wie schon gezeigt, bei Verletzungen der Informationssicherheit in Kommunikationsnetzen und -diensten häufig auftreten, führt in der Praxis dazu, daß keine oder lediglich eine meist geringe pauschale Kompensation verlangt wird.[563] Wenn in Netzen und Diensten vor allem so geartete Schäden auftreten und monetarisierbare, materielle Schäden relativ selten sind, kann der Anbieter auch unter der Verschuldenshaftung einen Anreiz haben, den geforderten Sorgfaltsstandard nicht zu erfüllen bzw. im Extremfall keinerlei Informationssicherheitsmaßnahmen zu ergreifen. Schließlich muß konstatiert werden, daß die Forschungsanreize im Bereich der Maßnahmen zur Sicherung der Informationssicherheit lediglich darin bestehen, den aktuellen Sorgfaltsstandard am kostengünstigsten zu erreichen. Eine Erreichung eines höheren Standards wird, wenn nicht vom Gesetzgeber verlangt, nicht angestrebt.[564]

Insgesamt kann also festgehalten werden, daß die Verschuldenshaftung für den Abbau der Informationsasymmetrie über die Informationssicherheit geeignet ist, wenn von einem gesetzlich geforderten Standard der Informationssicherheit ausgegangen werden kann, der dem optimalen Niveau entspricht, wenn der Verletzer der Informationssicherheit in den meisten Fällen zu identifizieren ist und wenn immaterielle Schäden nur begrenzt auftreten. Da jedoch sowohl der Schadenverursacher oft unbekannt als auch gemeinhin bei jedem Schadensfall auch eine immaterielle Nutzenkomponente beeinträchtigt wird, muß auch bei der Fähigkeit des Gesetzgebers, optimale Sorgfaltsniveaus zu definieren, von der Verschuldenshaftung bei Verletzungen der Informationssicherheit in Kommunikationsnetzen und -diensten abgesehen und die Gefährdungshaftung in Betracht gezogen werden.[565]

Unter dem Regime der Gefährdungshaftung muß der Schadenverursacher bzw. Anbieter in jedem Fall für den eingetretenen Schaden haften. Er wird deshalb das Niveau an Informationssicherheit wählen, das seine Gesamtkosten - die erwarteten

---

561 Vgl. dazu ebenda S. 60f, und Cansier (1993), S. 254f.

562 Vgl. dazu Endres (1991), S. 69f, S. 72 und S. 93. Bei einer Schadensüberschätzung wird er immer am geforderten Sorgfaltsstandard festhalten, weil er dadurch von der Haftung für jegliche Schäden befreit wird. Adams (1987), S. 14f, argumentiert, daß langfristig die Anbieter mit einer starken Risikofehlwahrnehmung aus dem Markt ausscheiden werden.

563 Vgl. dazu Cansier (1993), S. 259, und Endres (1991), S. 54f.

564 Vgl. zu der ambivalenten Wirkung der Verschuldenshaftung auf die Forschungsaktivitäten zur Verbesserung der Informationslage über das Schadenpotential Cansier (1993), S. 257ff.

565 Vgl. dazu auch Sieber (1995), S. 110ff.

Kompensationsforderungen plus die Kosten der installierten Informationssicherheitssysteme - minimiert, so daß es dadurch entsprechend der Optimalitätsbedingungen von Kapitel 2.5 zu einem Ausgleich von Grenznutzen und Grenzkosten von Informationssicherheitsmaßnahmen kommt. Die Informationsasymmetrie zuungunsten der Nachfrager wird abgebaut, weil die Anbieter keinen Anreiz haben, suboptimale Informationssicherheitsmaßnahmen in ihren Netzen und Diensten zu implementieren und die Teilnehmer im Schadensfall immer eine Kompensation erwarten können. Die üblichen Kritikpunkte an der Gefährdungshaftung, wie Moral Hazard von seiten der Nachfrager[566] und die Heterogenität der Nachfrager bezüglich ihres Schadenpotentials[567], sind bei der Informationssicherheit in Kommunikationssystemen nicht relevant. Denn die Teilnehmer haben keinen Anreiz, Informationssicherheitsverletzungen durch nachlässiges Verhalten herbeizuführen, weil damit oft auch immaterielle Nutzeneinbußen verbunden sind, die entweder überhaupt nicht oder nur mit einem geringen Pauschalbetrag kompensiert werden. Ferner kann durch die Gruppierung ähnlicher Teilnehmer in einem Netz bzw. Dienst auch deren Schadenpotential als nahezu homogen angesehen werden. Es muß aber auch hinsichtlich der Gefährdungshaftung geprüft werden, ob die bei der Verschuldenshaftung angesprochenen Mängel den Abbau der Informationsasymmetrien zwischen der Betreiber- und Teilnehmerseite behindern können.

Effizienzverluste wegen einer unzureichenden Sorgfaltsstandardfestsetzung durch den Gesetzgeber sind bei der Gefährdungshaftung nicht relevant, weil die Anbieter in jedem Fall zur Haftung herangezogen werden. Im Gegensatz zur Verschuldenshaftung, unter welcher die Anbieter i. d. R. immer den geforderten Sorgfaltsstandard einhalten, werden die Betreiber von Kommunikationsnetzen oder -diensten unter der Gefährdungshaftung ein suboptimales Informationssicherheitsniveau implementieren, wenn sie nach Eintreten von Schäden aufgrund nicht nachweisbarer Verursachung nicht immer zur Haftung herangezogen werden können.[568] Derselbe Effekt ist bei Haftungsbeschränkungen in den meisten Fällen zu erwarten.[569]

Beide Aspekte sind bei Verletzungen der Informationssicherheit in Kommunikationssystemen zu beobachten. Zum einen sind viele Kommunikationsvorgänge nicht nachvollziehbar, und es existieren vielfältige absichtliche Störungen durch unbekannte Dritte, so daß die Betreiber in vielen Fällen nicht als Verursacher identifi-

---

566 Vgl. dazu u. a. Buchanan (1970) und Oi (1973), S. 22f.
567 Vgl. dazu Adams (1987), S. 6f.
568 Vgl. dazu Endres (1991), S. 58ff.
569 Vgl. dazu ebenda S. 67ff und 71f.

ziert werden können. Zum anderen wirkt die mangelnde oder begrenzte Kompensation immaterieller Schäden wie eine Haftungsbegrenzung. Bei Risikounterschätzung durch den Anbieter kommt es zunächst zwar auch zu suboptimalen Aufwendungen[570] im Bereich der Informationssicherheit, jedoch werden die Betreiber im Zeitablauf durch die unverhältnismäßig vielen Schadensfälle realisieren, daß sie sich nicht im Kostenminimum befinden. Deshalb werden sie eine Ausdehnung ihrer Sicherheitsmaßnahmen vornehmen, so daß durch das Gewinnstreben der Netz- und Dienstebetreiber eine Selbstkorrektur bei unzureichenden Sicherheitsmaßnahmen stattfindet.[571]

Dieser Anpassungsmechanismus wirkt bei Verletzungen der Informationssicherheit nur eingeschränkt. Denn auch den Betreibern von Kommunikationssystemen werden nicht alle Schadensfälle bekannt, ferner können durch die von der hohen Komplexität der Netze und Dienste verursachte starke Korrelation der Schadensfälle in manchen Situationen Unfälle mit katastrophalen Ausmaß eintreten, die die Zahlungsunfähigkeit und damit den Konkurs des Betreibers bedeuten. Unter der Gefährdungshaftung führt dies im Vergleich zur Verschuldenshaftung dazu, daß besonders Katastrophenbegrenzungsmaßnahmen im Bereich der Informationssicherheit bei hohen Eintrittswahrscheinlichkeiten eher vernachlässigt werden.[572]

Schließlich werden durch einen Übergang zur Gefährdungshaftung die Forschungsbemühungen im Bereich der Schadenpotentiale durch Verletzungen der Informationssicherheit und der Informationssicherheitsmaßnahmen verstärkt werden, weil die dadurch gewonnenen Erkenntnisse unmittelbar zu einem verbesserten und damit gewinnsteigernden Sicherheitsniveau führen können. Die Bemühungen, innovative Kommunikationsnetze und -dienste auf den Markt zu bringen, werden dagegen gehemmt, weil die Betreiber einer hohen Unsicherheit über das mit ihnen verbundene Schadenpotential unterliegen, was bei einer Unterschätzung durch die hohen Entschädigungsforderungen zur Zahlungsunfähigkeit führen kann.[573]

Obwohl die Gefährdungshaftung nicht den Effizienzverlusten durch eine unzureichende Sorgfaltsstandardsetzung unterliegt und umfangreichere Forschungsaktivitäten auslöst, aus denen verbesserte Informationssicherheitsstandards hervorgehen werden, sind dennoch auch eine Reihe von Effizienzeinbußen zu verzeichnen.

---

570 Vgl. dazu ebenda S. 90ff.
571 Vgl. dazu Adams (1987), S. 14f.
572 Vgl. dazu allgemein Cansier (1993), S. 261.
573 Vgl. dazu auch das System Security Study Committee u. a. (1991), S. 167f.

Wenn die Anbieter in vielen Fällen nicht als Schadenverursacher identifiziert werden können, werden sie ihre Präventionsmaßnahmen begrenzen. Diesem Problem kann durch eine Umkehr der Beweispflicht begegnet werden, indem die Betreiber von Kommunikationsnetzen und -diensten beweisen müssen, daß sie nicht für den Schadensfall verantwortlich sind. Gravierendere Nachteile sind durch die Vernachlässigung immaterieller und katastrophaler Schäden bei der Ergreifung von Informationssicherheitsmaßnahmen zu erwarten, weil keine finanziellen Kompensationen entrichtet werden müssen bzw. können. Man sollte nun nicht eine Beibehaltung der Verschuldenshaftung in Erwägung ziehen, die zumindest die Einhaltung des gesetzlich geforderten Sorgfaltsstandards sicherstellt. Denn die Kombination der Gefährdungshaftung mit gesetzlich obligatorischen Mindestsicherheitsstandards kann die Vorteile der Gefährdungshaftung und der Verschuldenshaftung simultan realisieren.[574]

2.7.3.3 Verschuldens- versus Gefährdungshaftung der Betreiber von Kommunikationsnetzen und -diensten zur Internalisierung negativer Externalitäten

Wie gezeigt, ist die Produzenten- bzw. Produkthaftung der Betreiber von Kommunikationsnetzen und -diensten speziell auf den Abbau der Informationsasymmetrien zwischen Angebots- und Nachfragerseite ausgerichtet. Dagegen eignet sich das allgemeine Recht unerlaubter Handlungen, die für die übrigen Gesellschaftsmitglieder negativen Externalitäten von Verletzungen der Informationssicherheit abzubauen, die durch die Nutzung von Kommunikationssystemen hervorgerufen werden. Grundsätzlich müßte sowohl die Haftung der Netz- und Dienstebetreiber als auch der Nutzer von Kommunikationsnetzen und Diensten diskutiert werden. Da aber durch die ganze Analyse der Informationssicherheit in Kommunikationssystemen hindurch von der Annahme ausgegangen wurde, daß die Nutzer bzw. Teilnehmer zu keinen eigenständigen Maßnahmen zur Sicherung der Informationssicherheit fähig sind, werden sie die von Dritten erhobenen Haftungsansprüche an die Netz- und Dienstebetreiber weiterleiten.[575] Obwohl in Abschnitt 2.6.3.2 der Schwerpunkt auf die Externalitäten zwischen Netz- und Diensteteilnehmern und indirekt betroffenen Nicht-Teilnehmern gelegt wurde, wird sich in diesem Ab-

---

[574] In Abschnitt 2.7.5 werden Mindestsicherheitsstandards für die Gewährleistung der Informationssicherheit in Kommunikationsnetzen ausführlich diskutiert. Vgl. allgemein dazu Shavell (1984).

[575] In der Realität liegen die Fehlerursachen natürlich auch bei den Anwendern. Jedoch können die aus der Untersuchung der Haftung der Netz- und Dienstebetreiber abgeleiteten Ergebnisse unmittelbar auf die Nutzer von Netzen und Diensten übertragen werden.

schnitt auf die Untersuchung der Verschuldens- und Gefährdungshaftung der Netz- und Dienstebetreiber zur Internalisierung der negativen externen Effekte beschränkt.

Analog zur Wirkung der Verschuldenshaftung im Rahmen der Produzentenhaftung sorgt die allgemeine Haftung bei unerlaubten Handlungen dafür, daß die Betreiber von Kommunikationsnetzen und -diensten den vom Gesetzgeber geforderten Sorgfaltsstandard für die Informationssicherheit - sofern nicht zu anspruchsvoll - einhalten, weil sie sich damit von allen Haftungsansprüchen befreien. Wenn dieser Sicherheitsstandard über dem freiwillig gewählten Niveau an Informationssicherheit liegt, kann dadurch in der Regel eine Reduktion der negativen externen Effekte erreicht werden. In bezug auf Abbildung 21 auf S. 221 bedeutet dies, daß eine vollständige Internalisierung der externen Effekte nur dann realisiert wird, wenn der vorgegebene Standard an Informationssicherheit mindestens r^*_{sozial} beträgt.

Die Schwierigkeit besteht schließlich vor allem darin, die optimalen Sorgfaltsstandards r^*_{sozial} festzulegen, wobei je nach den Eigenschaften - Teilnehmerzahl n^* und Integrationsgrad I^* - des Kommunikationssystems verschiedene Niveaus angebracht sind. Denn, wie auch schon bei der Analyse der Produzentenhaftung dargelegt, sind umstrittene Bestimmung des Schadenfallverursachers, Fehleinschätzung der Schadenpotentiale durch den Schädiger, Haftungsbegrenzungen und Zahlungsunfähigkeit des Täters als Ursachen der Ineffizienzen bei der Verschuldenshaftung weniger relevant. Zumal in den meisten Fällen die Haftungsbefreiung durch Einhaltung des Sorgfaltsstandards die kostengünstigste Strategie ist. Jedoch muß eingeräumt werden, daß durch die fehlende vertragliche Beziehung zwischen Opfer und Verursacher die Quote der erfolgreichen Durchsetzung von Haftungsansprüchen geringer ausfallen wird als im Rahmen einer Anbieter-Nachfrager-Beziehung. Des weiteren können im Bereich der Verletzungen der Informationssicherheit die durch die schwierige Monetarisierung bedingte nicht durchgeführte Kompensation immaterieller Schäden und die bei katastrophalen Schadensfällen drohende Zahlungsunfähigkeit[576] dazu führen, daß gerade die Sorgfaltsstandards bezüglich des Vertraulichkeits- und des Katastrophenschutzes, also sowohl die Chiffrierung als auch die Implementation von Redundanzen, eher vernachlässigt werden. Schließlich erzeugt die Verschuldenshaftung bei den Netz- und Dienstebetreibern auch

---

576 In der Realität handelt es sich bei den Kommunikationssystemebetreibern um Großkonzerne mit beträchtlichem Eigenkapital, so daß selbst bei Schadensfällen mit hohen Kompensationsforderungen keine Zahlungsunfähigkeit droht und damit unter der Verschuldenshaftung der geforderte Sorgfaltsstandard eingehalten wird. Vgl. dazu allgemein Cansier (1993), S. 261.

keine zusätzlichen Forschungsanreize im Bereich der Informationssicherheit, die zu einer Erhöhung des Sicherheitsniveaus und damit auch zu einer verstärkten Internalisierung der negativen Externalitäten beitragen könnten.

Unter der Gefährdungshaftung werden die Netz- und Dienstebetreiber bei der Bestimmung ihren Aufwendungen für Informationssicherheitssysteme auch die möglichen Schäden für Dritte mit einbeziehen, weil sie in jedem Fall für die von ihnen verursachten Schäden haften müssen. Im Idealfall wird in jedem Kommunikationssystem das volkswirtschaftlich optimale Sicherheitsniveau r^*_{sozial} realisiert und damit eine vollständige Internalisierung der negativen Externalitäten erreicht. Jedoch gibt es - analog zur Gefährdungshaftung - im Rahmen der Produkthaftung, eine Reihe von Gründen, die ein geringeres Informationssicherheitsniveau erwarten lassen.

Wie schon angesprochen, wird die fehlende vertragliche Beziehung zwischen Opfer und Schädiger zu einer geringeren Erfolgsquote bei der Durchsetzung der Kompensationsforderungen führen. Diese Reduktion der erwarteten Kompensationszahlungen wird genauso wie eine durch Unkenntnis verursachte Unterschätzung des Schadenpotentials und die Haftungseinschränkung bei immateriellen Schäden sich unmittelbar in einem Informationssicherheitsniveau niederschlagen, das geringer ausfällt als das volkswirtschaftlich effiziente Ausmaß. Ferner führt die bei katastrophalen Unfällen durch immense Schadenskompensationsforderungen drohende Zahlungsunfähigkeit unter der Gefährdungshaftung in jedem Fall zu einer Senkung des Informationssicherheitsniveaus. Dagegen kann in der dynamischen Betrachtung mit einem höheren Informationssicherheitsniveau gerechnet werden, weil starke Forschungsanreize hinsichtlich der Bestimmung des wahren Schadenpotentials und der Verbesserung der Informationssicherheitstechnik bestehen.

Analog zur Untersuchung der Produkthaftung sollte trotz der Defizite der Gefährdungshaftung nicht die Verschuldenshaftung vorgezogen werden. Denn auch bei nicht vertraglichen Beziehungen zwischen Opfer und Schadenverursacher können durch die Kombination der Gefährdungshaftung mit gesetzlich obligatorischen Mindestsicherheitsstandards die Vorteile der Gefährdungshaftung und der Verschuldenshaftung simultan realisiert und eine umfangreichere Internalisierung der negativen Externalitäten von Verletzungen der Informationssicherheit in Kommunikationsnetzen erreicht werden.[577]

---

[577] Vgl. zu den Mindestsicherheitsstandards Abschnitt 2.7.5.

2.7.3.4 Die allokative Bewertung der aktuellen Haftungsbestimmungen der TKV und des BDSG

Obwohl die Regelungen des ProdHaftG nicht für Kommunikationsdienstleistungen gelten, weil diese kein Produkt im Sinne des ProHaftG darstellen[578], sieht die Neufassung der Telekommunikationsverordnung TKV eine Haftung der Deutschen Telekom AG vor. Nach §17 TKV haftet die Deutsche Telekom AG für Gesundheits-, Sach- und Vermögensschäden, die Teilnehmer oder sonstige am Fernmeldeverkehr Beteiligte durch die Nutzung ihrer Monopoldienstleistungen erleiden, wenn diese vorsätzlich oder fahrlässig verursacht worden sind. Obwohl die Beweislast bei der Deutschen Telekom AG liegt, wenn umstritten ist, ob sie den Schaden verschuldet hat, handelt es sich hier um Verschuldenshaftung. Überdies ist bei fahrlässigem Verschulden eine Haftungsbegrenzung von zwölftausend Deutsche Mark festgesetzt, und es werden alle weitergehenden Schadensersatzansprüche ausgeschlossen.[579]

Neben den allgemeinen Haftungsbestimmungen der TKV zeichnen sich Netz- und Dienstebetreiber dadurch aus, daß sie für die Berechnung der von ihnen erbrachten Leistung teilnehmerbezogene Daten erheben müssen. Ferner übermitteln eine Reihe von Anwendern wie Krankenhäuser und Ärzte personenbezogene Daten. Für beide Gruppen gelten hinsichtlich der Kompensation von dadurch verursachten Schäden §7 und §8 des BDSG.[580] Handelt es sich bei dem Schadenverursacher um eine öffentliche Stelle nach §2 BDSG, dann gilt nach §7 BDSG die Gefährdungshaftung mit einer Haftungsbegrenzung von zweihundertfünfzigtausend Deutschen Mark, wobei bei schweren Verletzungen des Persönlichkeitsrechtes auch Schäden, die nicht Vermögensschäden, also auch immaterielle Schäden, darstellen, angemessen in Geld ersetzt werden.[581] Für nicht-öffentliche Stellen nach §2 BDSG gilt dagegen Verschuldenshaftung, wobei die Beweislast beim Schädiger liegt.

Für alle übrigen Schadensfälle gilt die Schadenersatzpflicht des §823 BGB des Deliktrechtes, wonach der Schadenverursacher nur bei Vorsätzlich- oder Fahrlässigkeit zum Schadenersatz verpflichtet wird und damit wiederum das Prinzip der Verschuldenshaftung Gültigkeit hat. Außerdem ist nach §253 BGB eine Entschädi-

---

578 Vgl. dazu Büchner (1992), S. 110f.

579 Nach dem Regulierungsentwurf des Bundesministeriums für Post und Telekommunikation (1995), S. 14, soll im neuen Telekommunikationsgesetz der Verbraucherschutz explizit berücksichtigt werden.

580 Vgl. dazu BGBl. S. 2954 vom 20. 12. 1990.

581 Vgl. dazu Schadow (1991), S. 459f.

gung für Schäden, die immaterielle Schäden bzw. nicht Vermögensschäden sind, keine Ersatzpflicht vorgesehen.

Mit Ausnahme der Gefährdungshaftung öffentlicher Stellen bei Verletzungen des Datenschutzes haften sowohl nach der TKV als auch nach dem BDSG die Netz- und Dienstebetreiber und die sonstigen an Kommunikationssysteme angeschlossenen Verarbeiter personenbezogener Daten nach den Prinzipien der Verschuldenshaftung, wobei für gewöhnlich eine Entschädigung immaterieller Schäden nicht vorgesehen ist. Es ist deshalb nach der vorangegangenen Analyse des Haftungsrechtes zu erwarten, daß der vom Gesetzgeber geforderte Sorgfaltsstandard hinsichtlich der Informationssicherheit in Kommunikationssystemen realisiert wird. Jedoch muß dieser nach §21 TKV lediglich dem Stand der technischen Entwicklung entsprechen. Nach der Anlage zu §9 Satz 1 BDSG müssen Maßnahmen getroffen werden, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind, zu verhindern, daß bei deren Übertragung diese unbefugt gelesen, kopiert, verändert oder gelöscht werden können, wenn dies in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.[582] Aus beiden Paragraphen läßt sich nicht ableiten, welche Informationssicherheitsmaßnahmen nun im Einzelfall konkret zu treffen sind, so daß den Netz- und Dienstebetreibern und Datenverarbeitern ein relativ großzügiger Handlungsspielraum verbleibt, den sie zu ihren Gunsten, d. h. kosten- und deshalb wohl auch sicherheitsminimierend, ausschöpfen werden. Nur wenn ihnen in vielen Schadensfällen Fahrlässigkeit nachgewiesen werden kann und die Gerichte sie zu spürbaren Schadensersatzzahlungen verpflichten, werden in Kommunikationsnetzen und -diensten Informationssicherheitssysteme implementiert werden, die dem volkswirtschaftlich effizienten Sicherheitsniveau nahekommen.[583] Allerdings wird es den Opfern von Verletzungen der Informationssicherheit in Anbetracht der Komplexität von Kommunikationssystemen nur in wenigen Fällen möglich sein, die Netz- und Dienstebetreibern eines fahrlässigen Verhaltens zu überführen. Die Folge ist, daß sich nur ein sehr niedriges, weit vom volkswirtschaftlich Optimum entferntes Niveau an Informationssicherheit einstellen wird.

Die Untersuchung der bestehenden Haftungsbestimmungen hinsichtlich der Gewährleistung der Informationssicherheit hat erhebliche allokative Ineffizienzen aufgezeigt, die vor allem auch angesichts der Expansion des Informations- und Kommunikationssektors zu beträchtlichen volkswirtschaftlich Wohlfahrtsverlusten

---

582 Vgl. zu einer Diskussion des Verhältnismäßigkeitsprinzips von §9 BDSG Volle (1995).

583 Bis dies im Zeitablauf erreicht wird, sind aber gravierende Wohlfahrtsverluste zu verzeichnen.

führen werden. Dies rechtfertigt den Entwurf eines eigenständigen Informationssicherheitshaftungsgesetzes oder zumindest seine Berücksichtigung im allgemeinen und neu zu verfassenden Telekommunikationsgesetz. Welche grundsätzliche Regelungen dieses nach allokativen, aber auch distributiven und administrativen Gesichtspunkten enthalten sollte, wird im folgenden Abschnitt dargelegt.

2.7.3.5 Grundprinzipien eines Informationsicherheitshaftungsgesetzes

Da die Problematik der Informationssicherheit in Kommunikationssystemen starke Parallelen zur Umweltproblematik aufweist und, wie aufgezeigt, kein generelles Haftungsrecht hinsichtlich Verletzungen der Informationssicherheit existiert, werden hier einige Grundprinzipien vorgestellt, denen ein solches Informationssicherheitshaftungsgesetz aus allokativen, distributiven und administrativen Gründen genügen sollte.[584] Trotz der dargelegten Defizite ist aus allokativen Gesichtspunkten eine strikte verschuldensunabhängige Gefährdungshaftung vorzuziehen.[585] Denn Allokationsineffizienzen und Verteilungsungerechtigkeiten zwischen den Teilnehmern aufgrund Moral Hazard und Heterogenität des individuellen Schadenpotentials sind nicht zu erwarten.[586] Um eine Beweiserleichterung für geschädigte Teilnehmer und Dritte zu erreichen, sollte das Prinzip der Ursachenvermutung aus §6 des Umwelthaftungsgesetzes (UmweltHG) übernommen werden, wonach bereits dann für einen Schaden gehaftet werden muß, wenn berechtigt vermutet wird, daß ein bestimmtes Kommunikationssystem eine Informationssicherheitsverletzung verursacht hat. Jedoch sollte im Gegensatz zum UmweltHG die Beweislast beim potentiellen Verursacher liegen, denn der Geschädigte ist angesichts der Komplexität von Kommunikationsnetzen und -diensten in aller Regel nicht in der Lage, einen Indizienbeweis über den Schadenshergang zu führen.[587] Immaterielle Schäden sollten mit einem Pauschalbetrag abgegolten werden[588], weil damit die Betreiber von Kommunikationsnetzen und -diensten zusätzliche Anreize zu Präventionsmaß-

---

[584] Obwohl dieses Gesetz die Aktivitäten aller informationsverarbeitenden Institutionen umfassen sollte, wird sich in diesen Ausführungen lediglich auf die Haftungsproblematik der Betreiber von Kommunikationsnetzen und -diensten beschränkt.

[585] Diese sollte jedoch nicht wie im §6 des UmweltHG bei „Normalbetrieb" außer Kraft gesetzt werden. Vgl. zu diesem Kritikpunkt am UmweltHG Wacker-Theodorakopoulos & Kreienbaum (1991), S. 425f.

[586] Vgl. dazu die Ausführungen in Abschnitt 2.7.3.2.

[587] Hiermit wird die Problematik ungeklärter Verantwortlichkeiten zwischen Netz- und Dienstebetreibern und auch zwischen informationsverarbeitenden Kommunikationsteilnehmern auf diese übertragen.

[588] Für die Aufnahme des Schadensersatzes für immaterielle Schäden in das ProdHaftG plädiert auch Büchner (1992), S. 112.

nahmen vor allem im Bereich des Vertraulichkeitsschutzes erhalten und potentielle Opfer nicht zur Schadensherbeiführung verlockt und übermäßig Schadensersatzprozesse anstreben werden. Schließlich sollte der Gefahr der Zahlungsunfähigkeit bei katastrophalen Schadensfällen, denen Netz- und Dienstebetreiber ausgesetzt sind, mit der Verpflichtung zur Deckungsvorsorge begegnet werden. In Analogie zu §19 des UmweltHG kann dies mit dem obligatorischen Abschluß einer Haftpflichtversicherung[589] erreicht werden, wobei die zu entrichtenden Prämien nach den Risikopotentialen der verschiedenen Kommunikationssysteme zu bemessen sind.[590]

Unter distributiven Gesichtspunkten ist die Gefährdungshaftung insoweit günstig, als daß alle Kommunikationsteilnehmer aufgrund der verstärkt zu ergreifenden Sicherheitsmaßnahmen oder der für die abzuschließende Haftpflichtversicherung zu entrichtenden Prämien mit höheren Anschluß- oder Nutzungskosten belegt werden, aber dafür eine vollständige Kompensation im Schadensfall erwarten können. Die Gefährdungshaftung bringt also eine Vollversicherung der Kommunikationsteilnehmer mit sich, die bei risikoaversen Individuen nutzensteigernd wirkt und aufgrund der in Abschnitt 2.5.5.5 festgestellten Unvollständigkeit des Versicherungsangebotes zu begrüßen ist. Dagegen einzuwenden ist, daß für immaterielle Werte nach Abschnitt 2.5.5.4 von seiten risikoaverser Individuen keine Versicherungsnachfrage besteht und durch eine Gefährdungshaftung, die diese Schäden miteinbezieht, ein nutzensenkender Versicherungszwang eingeführt wird.[591] Durch die begrenzte pauschale monetäre Entschädigung immaterieller Schäden fällt aber letzterer negativer Aspekt nicht so stark ins Gewicht, und die Netz- und Dienstebetreiber haben dennoch einen Anreiz, Informationssicherheitsmaßnahmen verstärkt im Bereich des Vertraulichkeitsschutzes zu ergreifen. Verteilungsungerechtigkeiten zwischen den Teilnehmern innerhalb der verschiedenen Kommunikationsnetze aufgrund heterogenen Schadenpotentials sind durch ihre Homogenität eher unbedeutend.[592]

Hinsichtlich der Kosten der durch die Gefährdungshaftung verursachten Rechtsverfahren für die Gesellschaft ist einzuräumen, daß die durch Rechtsstreite zwischen

---

589 Diese könnte nach den Prinzipien der Software-Haftpflichtversicherung konzipiert werden. Vgl. Schulze Schwienhorst (1995). Vgl. zur Haftpflichtversicherung bei Umweltrisiken Cansier (1993), S. 270-280.

590 Die Prämien sollten also mit umfangreicheren Teilnehmergruppen n^* und höheren Integrationsgraden I^* zunehmen.

591 Vgl. zu diesem nicht lösbaren Konflikt Adams (1987), S. 22.

592 Vgl. zu den distributiven Ungerechtigkeiten bei heterogenen Konsumenten Abschnitt 1.5.3.4 oder Adams (1987), S. 6ff.

Netz- und Dienstebetreibern und Teilnehmern entstehenden Kosten ungerechtfertigter Weise auf die ganze Gesellschaft überwälzt werden. Dagegen ist es angemessen, daß die Gesellschaft die Kosten der Gefährdungshaftung zur Internalisierung der negativen Externalitäten von Verletzungen der Informationssicherheit übernimmt, weil potentiell alle Gesellschaftsmitglieder davon betroffen sein können. Insgesamt sind daher durch die Gefährdungshaftung im Rahmen eines Informationssicherheitshaftungsgesetzes keine gravierenden Verteilungsungerechtigkeiten zu erwarten.

Betrachtet man die schon angesprochenen administrativen Folgekosten einer solchen Ausgestaltung des Informationsicherheitshaftungsgesetzes, dann wird durch die Gefährdungshaftung die Gesamtzahl der erhobenen Rechtsansprüche umfangreich sein. Jedoch werden die Kosten pro Schadensfall gering ausfallen, weil lediglich die Netz- und Diensteanbieter beweisen müssen, daß sie den Schaden nicht verursacht haben. Da die Gefährdungshaftung in der dynamischen Entwicklung ein höheres Niveau an Informationssicherheit in Kommunikationsnetzen hervorbringen wird, reduziert sich folglich auch die Anzahl der vorgebrachten Klagen, so daß langfristig die Kosten der Gefährdungshaftung für das Rechtssystem günstig eingeschätzt werden können.

2.7.4 Die Subventionierung von Informationssicherheitssystemen in Kommunikationsnetzen und -diensten

2.7.4.1 Die Ziele der Subventionierung von Informationssicherheitssystemen

Während der unterbreitete Entwurf eines Informationsicherheitshaftungsgesetzes sowohl zum Abbau der Informationsasymmetrien zwischen Anbietern und Nachfragern von Kommunikationssystemen als auch zur Internalisierung der negativen Externalitäten von Informationssicherheitsverletzungen beitragen kann, ist die Intention der Pigou-Lösung vor allem letzteres Ziel.[593] Als mögliche Strategien kommen grundsätzlich die Subventionierung von Maßnahmen, welche die Informationssicherheit in Kommunikationssystemen fördern, und die Besteuerung von

593 Unter meritorischen Gesichtspunkten kann durch die Korrektur der ursprünglichen Marktpreise auch bei individueller Unterschätzung des durch Informationssicherheitsverletzungen hervorgerufenen Schadenpotentials eine Wohlfahrtserhöhung erreicht werden.

Aktivitäten, die negative externe Effekte bei Verletzungen der Informationssicherheit verursachen, in Betracht.

Allerdings bringt die Einführung einer Besteuerungslösung hinsichtlich der Informationssicherheit in Kommunikationssystemen eine Reihe theoretischer und praktischer Probleme mit sich. Wie schon in Abschnitt 1.5.4 deutlich wurde, kann durch die Besteuerung risikoreicher Aktivitäten nur deren Umfang und somit das Ausmaß der negativen Externalitäten reduziert, aber nicht unbedingt eine vollständige Internalisierung erreicht werden.[594] In der Besteuerungspraxis tauchen weitere elementare Schwierigkeiten bei der Festlegung der Bemessungsgrundlage und des Steuertarifes auf. Zwar ist der Umfang der Informationsflüsse innerhalb eines Kommunikationsnetzes oder -dienstes indirekt durch einen Rückgriff auf die Teilnehmerabrechnungen bestimmbar.[595] Aber schon die Kategorisierung der Kommunikationsinhalte nach der jeweiligen externen Schadenhöhe ist in der Praxis nicht durchführbar, weil jeder einzelne Kommunikationsvorgang daraufhin untersucht werden muß, ob und inwieweit eine Verletzung der Informationssicherheit auch unbeteiligte Dritte schädigen könnte. Außerdem müssen die bereits implementierten Informationssicherheitssysteme in der Höhe des Steuertarifes positiv berücksichtigt werden, dessen absolutes Niveau allerdings nur willkürlich ohne ökonomische Fundierung festgelegt werden kann. Die bei einer Erhebung anfallenden Kosten und die durch sie entstehenden Ungerechtigkeiten können die Einführung einer solchen Steuer nicht rechtfertigen, so daß sie in der weiteren Untersuchung nicht weiter betrachtet wird.[596]

Neben der problematischeren Besteuerungslösung scheint die Subventionslösung ein erfolgversprechender Ansatz zu sein. Deshalb wird zunächst die unmittelbare Subventionierung von Informationssicherheitssystemen in bereits bestehenden Kommunikationssystemen diskutiert, bevor auf die Problematik der kritischen Masse von Kommunikationsnetzen und -diensten zurückgegriffen und in diesem Zusammenhang die Subventionierung der Markteinführung von Netzen und Dien-

---

[594] Diese ist eigentlich nur bei einem prohibitiv hohen Steuersatz möglich, der zu einer Einstellung der mit externen Risiken behafteten Aktivitäten führt, was im Fall der Kommunikationssysteme volkswirtschaftlich ineffizient und politisch nicht durchsetzbar ist.

[595] Das zukunftsträchtige Übertragungsverfahren Asynchroner Transfer Mode (ATM) ermöglicht schon eine exakte Bestimmung der übermittelten Informationsmenge. Vgl. Paszkowsky (1995).

[596] Eine solche Steuer kann auch die Expansion des Kommunikationsmarktes bremsen und die nationale Wettbewerbsfähigkeit beeinträchtigen, wobei durch die grenzüberschreitenden Wirkungen von Kommunikationsnetzen grundsätzlich eine internationale Lösung anzustreben ist.

sten mit qualitativ hochwertigen Informationssicherheitsmechanismen untersucht wird.

Da in der Bundesrepublik Deutschland durch das noch bestehende Monopol der Deutschen Telekom AG keine allgemeinen Subventionslösungen im Bereich der Informationssicherheit in Kommunikationssystemen existieren, können keine bestehenden Lösungen auf ihre ökonomische Effizienz untersucht werden, so daß dieser Abschnitt mit einer umfassenden Bewertung der vorgeschlagenen Subventionslösungen schließt.

2.7.4.2 Die Subventionierung von Informationssicherheitssystemen in vorhandenen Kommunikationsnetzen und -diensten

Im Gegensatz zur indirekten Reduzierung der negativen Externalitäten mittels Besteuerung der Informationsflüsse kann durch die Subventionierung von Informationssicherheitssystemen unmittelbar eine Erhöhung des Informationssicherheitsniveaus und eine Internalisierung der negativen externen Effekte erreicht werden. Abbildung 23 zeigt, daß durch eine Subventionierung der Grenzkosten von Informationssicherheitsmaßnahmen in Höhe des optimalen Subventionstarifs die Wohlfahrtsverluste durch die dargestellten Externalitäten vollständig verschwinden.

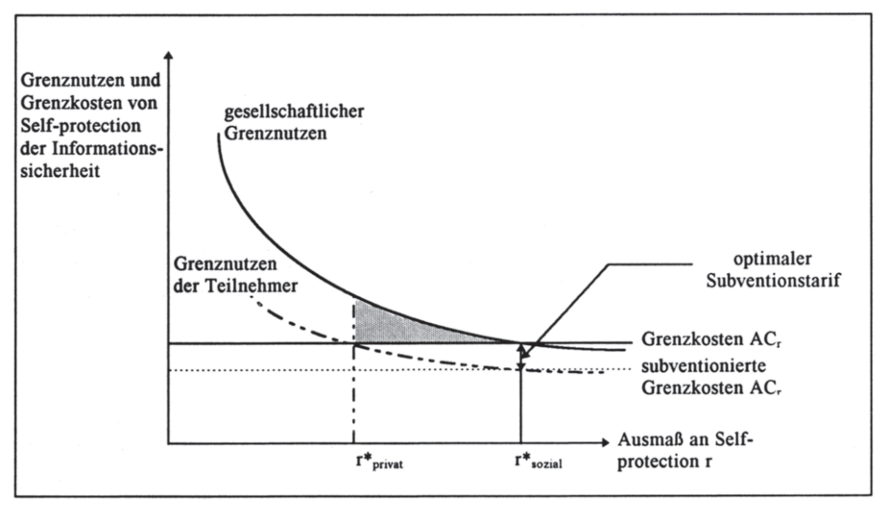


Abb. 23: Internalisierung externer Effekte von Informationssicherheitsmaßnahmen durch Subventionierung

Konkret wird das für die Gesellschaft optimale Präventionsniveau dadurch erreicht, indem sich die Subventionsempfänger - die Netz- und Dienstebetreiber[597] - nun geringeren Grenzkosten gegenübersehen und die Präventionsaufwendungen so weit ausdehnen, bis der Grenznutzen ihrer Kommunikationsteilnehmer gleich den subventionierten Grenzkosten ist. Die eigentliche Höhe des Subventionsbetrages für den einzelnen Netz- und Dienstebetreiber errechnet sich als Produkt aus Subventionsbemessungsgrundlage und Subventionstarif. Als Bemessungsgrundlage bieten sich die Aufwendungen für Maßnahmen zur Sicherstellung der Informationssicherheit, also zum Beispiel die Kosten für die Einrichtung eines Verschlüsselungssystems, an. Damit handelt es sich um eine Wertsubvention mit Empfangsauflage. Größere Schwierigkeiten bereitet die Bestimmung des Subventionstarifes, der sich im Idealfall, wie Abbildung 23 zeigt, als Differenz zwischen dem sozialen und dem teilnehmerspezifischen privaten Grenznutzen der Informationssicherheitsmaßnahmen bestimmt. Beide Größen sind in der Realität schwer zu quantifizieren, so daß in Kapitel 2.6 lediglich konstatiert werden konnte, daß der Differenzbetrag positiv von der Teilnehmerzahl n* und dem Integrationsgrad I* eines Kommunikationssystems abhängt. Diese Erkenntnis sollte zumindest in die qualitative Gestaltung des Subventionstarifes einfließen.[598]

Die Darstellung der Subventionslösung zeigt, daß es sich hierbei um einen in der Praxis durchaus durchführbaren Weg zur Internalisierung negativer Externalitäten handelt. Bevor eine Bewertung nach allokativen, distributiven und administrativen Aspekten erfolgt, wird noch eine weitere Subventionslösung aufgezeigt.

2.7.4.3 Die Subventionierung der Errichtung von Kommunikationsnetzen und -diensten mit hochwertigen Informationssicherheitseigenschaften

Neben der Subventionierung von Informationssicherheitssystemen in bereits bestehenden Kommunikationsnetzen und -diensten bietet sich im stark expandierenden und sich weiter differenzierenden Telekommunikationsmarkt eine weitere Strategie

---

[597] Grundsätzlich könnten die Subventionen auch an die einzelnen Teilnehmer mit der Bedingung ausgezahlt werden, daß sie nur Anschlüsse an Kommunikationssystemen mit bestimmten Mindestsicherheitsstandards hinsichtlich der Informationssicherheit wählen dürfen. Aus verwaltungstechnischen Gründen ist es jedoch günstiger, die Subventionen direkt an die jeweiligen Betreiber von Kommunikationssystemen auszuzahlen. Hier bietet sich entsprechend §7d Einkommensteuergesetz für Umweltschutzgüter auch eine erhöhte Abschreibung von Informationssicherheitssystemen an.

[598] Ferner sollten Informationssicherheitsmaßnahmen zum Schutz immaterieller Werte eine besondere finanzielle Unterstützung erfahren, weil wie aufgezeigt selbst die Gefährdungshaftung den Betreibern nur einen begrenzten Präventionsanreiz bietet.

an. Wie in Kapitel 2.4 verdeutlicht, wird sich ein Kommunikationssystem nur dann am Markt durchsetzen, wenn es sich mindestens aus einer bestimmten kritischen Masse n_k an Kommunikationsteilnehmern zusammensetzt. In den bisherigen Ausführungen wurden mögliche Strategien zur Erreichung dieser kritischen Masse n_k vernachlässigt.[599] Handelt es sich bei dem einzuführenden Kommunikationssystem um einen Dienst oder ein Netz, das ein sehr hohes Niveau an Informationssicherheit gewährleisten kann und damit selbst nur geringe negative Externalitäten, aber indirekt starke positive externe Effekte auslöst, weil eine Substitution weg von Systemen mit hohem externen Schadenpotential ausgelöst wird, dann sollte von seiten des Staates eine aktive finanzielle Unterstützung solcher „Hochsicherheits"-Systeme erfolgen.[600]

Abbildung 24 macht die positiven Externalitäten als Differenz zwischen dem gesellschaftlichen und dem teilnehmerspezifischen Nutzen eines Anschlusses an ein solches „Hochsicherheits"-Systems und den daraus folgenden Subventionsbedarf deutlich.

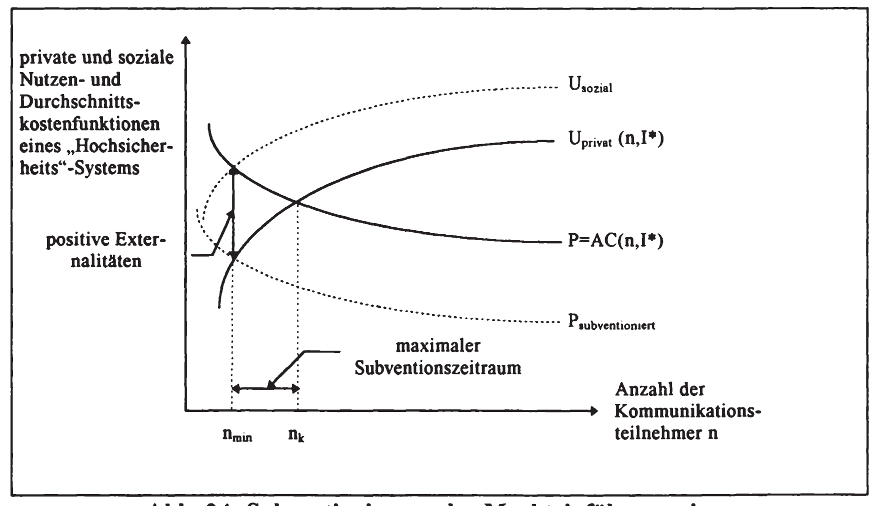


Abb. 24: Subventionierung der Markteinführung eines „Hochsicherheits"-Systems

599 Vgl. zu einer Übersicht Schoder (1995), S. 144-152.

600 Sind die Betreiber von Netzen und Diensten die Subventionsempfänger, dann handelt es sich hier um eine Subvention mit Verwendungsauflage, welche nur gewährt wird, wenn ein vorgeschriebener Mindestsicherheitsstandard erfüllt wird. In Abschnitt 2.7.4.4 wird problematisiert, ob Kommunikationssystembetreiber oder -teilnehmer Subventionsempfänger sein sollten.

Grundsätzlich sollte jeder Neuanschluß an dieses „Hochsicherheits"-System in Höhe der dadurch ausgelösten positiven Externalitäten subventioniert werden. Dieses Vorgehen zieht sowohl in zeitlicher als auch in quantitativer Hinsicht einen unbegrenzten Subventionsbedarf nach sich, der nicht einmal unbedingt eine erfolgreiche Markteinführung garantiert. Deshalb sollte zusätzlich zu den strengen Informationssicherheitseigenschaften ein Kommunikationssystem erst dann subventioniert werden, wenn eine Mindestteilnehmerzahl n_{min} erreicht worden ist, welche als Indikator für seine Durchsetzungsfähigkeit am Markt angesehen werden kann. Diese Mindestteilnehmerzahl n_{min} liegt zum einen unter der kritischen Masse n_k und zum anderen exakt dort, wo der gesellschaftliche Nutzen eines Teilnehmeranschlusses gleich den anfallenden Durchschnittskosten AC ist. Da letztere Teilnehmerzahl eigentlich nicht genau zu bestimmen ist, sollte die vom Betreiber zu quantifizierende kritische Masse n_k als Orientierungsgröße genommen und davon je nach implementierter Informationssicherheitstechnik ein Prozentsatz abgezogen werden. Der einmalige Subventionsbetrag pro Teilnehmer, der eigentlich mit den nicht zu quantifizierenden, positiven Externalitäten übereinstimmen sollte, kann als Prozentsatz, welcher der prozentualen Differenz zwischen kritischer Masse n_k und minimaler Teilnehmerzahl n_{min} entspricht, mal der jeweiligen Durchschnittskosten AC(n, I*) berechnet werden.[601] Der Subventionszeitraum erstreckt sich idealer Weise auf die Zeitspanne zwischen Erreichen der Mindestteilnehmerzahl n_{min} und der kritischen Masse n_k. Damit ist unmittelbar eine maximale Subventionssumme gewährleistet.[602]

Hiermit wurden zwei Subventionslösungen vorgestellt, die geeignet sind, die Informationssicherheit in Kommunikationsnetzen zu verbessern. Dabei setzt das erste Verfahren direkt am bestehenden Angebot an, während die zweite Strategie auf einer Umstrukturierung des bestehenden Angebots zu Kommunikationssystemen mit einem höheren Niveau an Informationssicherheit hinwirken will. Beide Vorgehensweisen werden im folgenden nach allokativen, distributiven und administrativ-fiskalischen Gesichtspunkten analysiert.

---

[601] Nehmen die positiven Externalitäten zu, dann steigen also sowohl Subventionsbetrag pro Teilnehmer als auch der maximale Subventionszeitraum.

[602] Diese Subventionssumme S berechnet sich wie folgt: $S = (n_k - n_{min}) \times [(n_k - n_{min})/n_k] \times AC(n, I^*)$.

2.7.4.4 Die Bewertung der vorgestellten Subventionslösungen

Grundsätzlich hängt der Grad der Allokationsverbesserung durch Subventionen davon ab, ob die Höhe des Subventionstarifs den positiven externen Effekten entspricht. Die Effizienz wird bei den beiden Subventionsvorschlägen u. a. wegen der problematischen Quantifizierung der Grenznutzen eher gering sein. Außerdem erhöhen zusätzliche Informationssicherheitssysteme nicht nur die Wohlfahrt der indirekt Betroffenen, sondern generell auch die der Kommunikationsteilnehmer, so daß die Bestimmung der reinen positiven Externalitäten eigentlich nicht möglich ist. Dennoch kann eine Subventionierung der Installation von Informationssicherheitsvorkehrungen in bereits vorhandenen Kommunikationssystemen zu einer Erhöhung der Informationssicherheit führen. Dagegen ist die finanzielle Unterstützung der Markteinführung von „Hochsicherheits"-Systemen trotz der Restriktion durch eine Mindestteilnehmerzahl n_{min} mißlungen, wenn die kritische Masse an Teilnehmern n_k durch fehlendes Interesse von seiten der Nachfrager nicht erreicht wird. Deshalb sollte diese Strategie auch auf die Expansionsphase[603] des Telekommunikationsmarktes beschränkt werden, weil Kommunikationsteilnehmer Netze und Dienste, die sie eine lange Zeit erfolgreich genutzt haben, nur bedingt verlassen werden.[604]

Ferner haben die Subventionsempfänger einen Anreiz, das Durchschnittskostenniveau AC zu übertreiben, um damit einen relativ hohen Subventionstarif über einen - bedingt durch eine große kritische Masse n_k - langen Subventionszeitraum zu erhalten. Jedoch hat dieser Lösungsweg den Vorteil, daß Informationssicherheitsmaßnahmen schon beim Aufbau eines Netzes oder Dienstes installiert werden und damit im Gegensatz zur Subventionierung vorhandener Kommunikationssysteme zunächst keine zusätzlichen Nachrüstungskosten anfallen. Generell herrscht in Kommunikationsnetzen und -diensten nämlich das Problem, daß ein erheblicher Anteil der Sachkapitalinvestitionen irreversibel, im Sinne fehlender Verwendungsmöglichkeiten in anderen Einsatzfeldern ist, so daß eine Nachrüstung u. U. mit bereits installierter Hard- und Software nicht kompatibel ist. Die Subventionierung der Nachrüstung von Informationssicherheitssystemen wird bei starken Irreversibilitäten von den Netz- und Dienstebetreiber nicht in Anspruch genommen wer-

---

603 Für die Bundesrepublik Deutschland bietet sich diese Vorgehensweise deshalb vor allem in den ersten Jahren nach der Liberalisierung des Telekommunikationsmarktes an.

604 Vgl. zur Problematik der staatlichen Regulierung des Übergangs von einem bestehenden auf ein neues hochwertigeres Netz Blankart & Knieps (1992), S. 82ff.

den.[605] Bei beiden Strategien muß negativ angemerkt werden, daß im Laufe der Zeit vor allem durch die vorsätzlichen Gefährdungen durch kriminelles Potential weiterer Subventionsbedarf entsteht, weil die bestehenden Informationssicherheitsmechanismen auf das sich ändernde Bedrohungspotential ausgerichtet werden müssen.

Die Verteilungseffekte der beiden Subventionsstrategien, welche sich in einer Verbilligung der Informationssicherheitssysteme niederschlagen, sind durch ihre positiven Externalitäten erwünscht. Während bei der Subventionierung vorhandener Kommunikationssysteme deren Teilnehmer in gleichem Maße in den Genuß der höheren Informationssicherheit kommen, sind die distributiven Effekte bei der begrenzten Subventionierung von „Hochsicherheits"-Systemen in der Markteinführungsphase ungleicher. Obwohl die finanzielle Unterstützung erst ab einer Mindestteilnehmerzahl n_{min} einsetzt, wird der Netz- oder Dienstebetreiber diese bereits in der Startphase in seine Preisgestaltung miteinbeziehen, so daß schon die ersten Teilnehmer in den Genuß der Verbilligung des Netzanschlusses kommen werden. Diejenigen Teilnehmer, die nach dem Erreichen der kritischen Masse sich einem „Hochsicherheits"-System anschließen, werden nicht mehr von einem subventionierten Netzanschluß begünstigt werden, obwohl auch sie durchaus noch positive Externalitäten hervorrufen. Diese offenbar ungleiche Verteilung von Subventionsleistungen kann aber dadurch legitimiert werden, daß „Früheinsteiger" in ein „Hochsicherheits"-System einem höheren „Flop-Risiko" unterliegen.[606] Insgesamt weisen beide Subventionslösungen also beabsichtigte Verteilungseffekte auf.

Schließlich muß noch eine Einschätzung der fiskalischen und administrativen Kosten der Subventionierung von Informationssicherheitssystemen erfolgen. Obwohl die unmittelbare finanzielle Belastung beider Subventionslösungen trotz restriktiver Ausgestaltung für den Staat hoch ist, sind die indirekten administrativen Kosten gering, wenn die Netz- und Dienstebetreiber die Subventionen direkt bzw. über steuerliche Begünstigungen erhalten.[607] Denn sowohl die Ausgaben für Informationssicherheitsmaßnahmen als auch die Anzahl der Neuanschlüsse können ohne großen Verwaltungsaufwand ermittelt werden. Außerdem kann ein Teil der Sub-

---

[605] Vgl. allgemein zur Irreversibilitätsproblematik in Kommunikationssystemen Knorr (1993), S. 112ff, und speziell zur Informationssicherheit Kowalski & Wolfenstetter (1994), S. 36.

[606] Vgl. zur Rückentwicklung und zum „Flop" von Telekommunikationsdiensten Schoder (1995), S. 25-34.

[607] Vgl. auch Fußnote 597. Eigentlich kommen nur bei der zweiten Subventionslösung auch die Kommunikationsteilnehmer als Subventionsempfänger in Frage, wobei sich die gleichen allokativen Effekte bei höherem administrativem Aufwand einstellen.

ventionssumme für die Markteinführung von „Hochsicherheits"-Systemen nach einer erfolgreichen Etablierung vom Netz- oder Dienstebetreiber zurückgefordert werden, so daß es sich in einem solchen Fall um eine partielle Darlehenslösung handelt.

Trotz der relativ hohen direkten finanziellen Belastung des Staates kann durch die vorgeschlagenen Subventionslösungen eine gesamtwirtschaftliche Wohlfahrtssteigerung ohne negative Verteilungswirkungen und mit geringen administrativen Kosten erreicht werden, wenn die Kompatibilität der nachzurüstenden Informationssicherheitssysteme mit den bestehenden Systemkomponenten gegeben ist und die kritischen Massen an Teilnehmern in den „Hochsicherheits"-Systemen erreicht werden. Denn dann wird sich das angestrebte Niveau an Informationssicherheit in Kommunikationssystemen einstellen. Die Besteuerungslösung ist im Moment zwar noch schwer vorstellbar, weil Verletzungen der Informationssicherheit bisher in der gesamten Gesellschaft nur Einzelopfer trifft, die individuell mit einem geringeren Aufwand entschädigt werden können. Eine Besteuerung der in Kommunikationssystemen transportieren Informationen kann aus ökonomischen Gesichtspunkten gerechtfertigt werden, wenn folgende Bedingungen erfüllt sind. Zum einen muß sich die informations- und kommunikationstechnischen Gesellschaft so weiterentwickeln, daß alle Gesellschaftsmitglieder zu potentiellen Opfern von Verletzungen der Informationssicherheit werden. Zum anderen müssen die technischen Möglichkeiten eine genaue und kostengünstige Kategorisierung von Kommunikationsinhalten nach ihrem externen Schadenpotential erlauben.

2.7.5 Die Regulierung der Standardisierung von Kommunikationssystemen zur Gewährleistung der Informationssicherheit

2.7.5.1 Vorbemerkungen

Die Übereinkunft der verschiedenen Kommunikationsteilnehmer auf einen einheitlichen Standard ist die Grundvoraussetzung für das reibungslose Funktionieren aller Kommunikationsnetze und -dienste. Mit der Standardisierung sind aber auch unmittelbar Folgen für die Allokation und den Wettbewerb im Telekommunikati-

onssektor verbunden.[608] In diesem Abschnitt wird die Analyse aber lediglich darauf gerichtet, inwieweit durch eine Regulierung der Standardisierungsaktivitäten eine Allokationsverbesserung hinsichtlich der Informationssicherheit in Kommunikationssystemen erreicht werden kann.

Zunächst wird ein kurzer Überblick über die wichtigsten Standardisierungsgremien und ihre Bemühungen in bezug auf Verbesserungen der Informationssicherheit in Kommunikationsnetzen und -diensten gegeben. Daran anschließend wird dargelegt, welche Allokationsineffizienzen durch Verletzungen der Informationssicherheit mit Hilfe der Regulierung der Standardisierung vermindert werden können.[609] Durch die bevorstehende Liberalisierung des Telekommunikationsmarktes und die wenig konkrete Zielsetzung der staatlichen Regulierung im Bereich der Telekommunikation[610], welche lediglich die Berücksichtigung sozialer Belange und die Gewährung eines wirksamen Verbraucher- und Datenschutzes mittels möglichst marktkonformer, aber nicht näher bestimmter Maßnahmen verlangt, erscheint eine Analyse aktueller Regulierungsaktivitäten in der Bundesrepublik Deutschland nicht angebracht. Statt dessen werden generelle Regulierungsvorschläge gemacht, die sich auf die Besetzung der Normierungsgremien, auf die Anforderungen an die Standardisierungsergebnisse und auf deren Durchsetzung beziehen.[611] Der Abschnitt endet mit einer Bewertung der Regulierungsvorschläge hinsichtlich der Verbesserung der Informationssicherheit in Kommunikationssystemen.

2.7.5.2 Ein Überblick über die Standardisierungsaktivitäten im Bereich der Informationssicherheit in Kommunikationsnetzen und -diensten

Die aus der Normierung folgende Standardisierung der Hard- und Software im Telekommunikationsbereich ist für ein reibungsloses Funktionieren der Kommunika-

---

608 Vgl. dazu u. a. Besen & Saloner (1989), Kampmann (1993), Knorr (1993) und David & Steinmueller (1994).

609 Die Zielsetzung der Regulierung im Telekommunikationssektor wird gegenwärtig von wettbewerbs- und verteilungspolitischen Gesichtspunkten dominiert, wobei der Zugang aller Gesellschaftmitglieder zu allen Kommunikationsnetzen und -diensten („universal service") im Vordergrund steht. Vgl. dazu Tyler, Letwin und Roe (1995).

610 Vgl. §2, §9 und §10 des PTRegG, BGBl. S. 2371 vom 22. 9. 1994. Im Eckpunkte-Papier des Bundesministeriums für Post und Telekommunikation (1995) S. 15, wird auch ein völlig neues Telekommunikationsgesetz vorgesehen, dessen Gegenstand die allgemeine Regulierung der Telekommunikationsmärkte sein wird.

611 Diese Regulierung wird vor allem auch durch die zukünftige Zurückdrängung der bisher staatlichen Telekommunikationsmonopole aus den Regulierungsgremien notwendig.

tionsverbindungen unerläßlich.[612] Deshalb hat die internationale und globale Integration der Telekommunikationsbeziehungen einen immer weitergehenden Standardisierungsbedarf ausgelöst. Dieser Aufgabe haben sich privatrechtliche Institutionen, die einen Zusammenschluß von Anbietern und Nachfragern von Telekommunikationsleistungen darstellen und an dessen Spitze die „International Organization for Standardization" (ISO) steht, gewidmet. Andererseits beschäftigen sich auch öffentlich-rechtliche Gremien, die von den nationalen Fernmeldeverwaltungen dominiert werden und die sich auf der höchsten internationalen Ebene in der „International Telecommunication Union - Standardization" (ITU-S) vormals „International Telegraph and Telephone Consultive Committee" (CCITT) vereinigen, damit.[613] Beiden ist gemeinsam, daß sie zwar rechtlich nicht bindende Empfehlungen verabschieden, die jedoch faktisch verbindlichen Charakter haben. Während sich in der Vergangenheit die Tätigkeiten der CCITT vor allem auf die öffentlichen Telekommunikationssysteme und die der ISO auf Datenverarbeitung und -übermittlung gerichtet haben, hat sich aufgrund der Integration beider Bereiche bereits eine koordinierte Zusammenarbeit durchgesetzt.[614]

Auf europäischer Ebene wurde mit der Gründung des „European Telecommunication Standard Institute" (ETSI) neben den nationalen staatlichen Netz- und Dienstebetreibern auch den Herstellern von Kommunikationstechnik, privaten Netz- und Dienstebetreibern, Vertretungen von Kommunikationsteilnehmern Zugang zum Standardisierungsprozeß im Bereich der Telekommunikation gewährt.[615] Auf nationaler Ebene ist zur Zeit der neugegründete Regulierungsrat für die Entwicklung von Standards und Zulassungsvorschriften im regulierten Telekommunikationsbereich zuständig.[616]

Da die Erarbeitung von Informationssicherheitsstandards zur Zeit sowohl auf internationaler Ebene innerhalb der ISO nicht weiter verfolgt wird[617] als auch auf na-

---

612 Vgl. zu den Entwicklungsphasen, die von anfänglichen Normierungsaktivitäten bis hin zur faktischen Implementierung von Standards führen, im Bereich der Kommunikationstechnik in der EG, Höller (1993), S. 42f.

613 Vgl. die Übersichten der Standardisierungsinstitutionen in Knorr (1993), S. 119, und in Kampmann (1993), S. 55, sowie die umfassende und detaillierte Zusammenstellung von Macpherson (1990). Vgl. zur aktuellen Situation der ITU MacLean (1995).

614 Das von der ISO entwickelte Schichtenmodell OSI ist von der CCITT als Empfehlung für die Standardisierung von ISDN übernommen worden. Vgl. Knorr (1993), S. 164.

615 Vgl. zu einer deskriptiven Beschreibung der ETSI u. a. Kampmann (1993), S. 69ff.

616 Vgl. §§11ff des PTRegG, BGBl. S. 2371 vom 22. 9. 1994. Zu einer kritischen Betrachtung der Regulierungstätigkeiten in der Bundesrepublik Deutschland vgl. Knorr (1993), S. 168ff.

617 Vgl. dazu Kowalski & Wolfenstetter (1994), S. 31, und Pfitzmann & Rannenberg (1993), S. 177.

tionaler Ebene die Standardisierungsfunktion des Regulierungsrates bisher nur allgemein definiert worden ist, werden im folgenden zwei Normungsinstitutionen der ETSI im Bereich der Informationssicherheitssysteme für Kommunikationsnetze und -dienste kurz dargestellt.[618]

Das Subkomitee „Security Algorithms Group of Experts" (SAGE), gegründet 1991, hat auf Weisung der technischen Abteilung der ETSI vor allem die Aufgabe, Chiffriertechniken zu entwerfen und die Randbedingungen für ihre Implementierung in verschiedene Kommunikationsnetze und -dienste festzulegen. SAGE setzt sich ausschließlich aus den Delegierten der öffentlichen Netzbetreiber zusammen. Probleme ergeben sich jedoch dadurch, daß die erarbeiteten Regulierungsvorschläge für alle ETSI-Mitglieder, die nicht der EG angehören, nicht verbindlich sind und es deshalb mit den jeweiligen nationalen Institutionen zu Konflikten kommen kann.

Nach der Gründung von SAGE wurde sehr schnell deutlich, daß zwischen der Entwicklung von Informationssicherheitssystemen durch SAGE und deren Implementierung als Sicherheitsstandard in Kommunikationssystemen eine Lücke existiert, zu deren Schließung die Einrichtung einer weiteren Institution notwendig sein würde. „Security Technology Advisory Group" (STAG) soll diese Aufgabe bewältigen, indem sie u. a. den technischen Komitees zur Normierung von Kommunikationssystemen allgemeingültige Sicherheitsstrategien und Leitlinien zu deren Implementierung erarbeiten und vorgeben. Es werden also Bedrohungsanalysen durchgeführt, daraus Sicherheitsbedürfnisse abgeleitet, Anforderungen an Informationssicherheitssysteme formuliert, Regulierungsprobleme identifiziert und schließlich Sicherheitsstandards in allgemeine ETSI-Standards integriert. Im Gegensatz zu SAGE ist STAG ein offenes Komitee.[619]

Insgesamt kann festgehalten werden, daß Aspekte der Informationssicherheit in den Europäischen Telekommunikationsstandards durch die Einrichtung der Institutionen SAGE und STAG eine stärkere Berücksichtigung finden.

---

618 Vgl. zum folgenden und weiteren Sicherheitsinitiativen bei der Standardisierung in Kommunikationssystemen Kowalski & Wolfenstetter (1994), S. 31ff.

619 Schließlich existiert seit 1991 ein von der ETSI unabhängiges Beratungsgremium SOGIS („Senior Officials Group for Information Security"), das sich aus den Delegierten der nationalen Wirtschafts-, Innen- , Postministerien und anderen Institutionen zusammensetzt und sich mit Fragen der Import- und Exportbeschränkung und der Verfügbarkeit von Informationssicherheitssystemen befaßt. Vgl. Kowalski & Wolfenstetter (1994), S. 37f.

2.7.5.3 Die Ziele von Mindestsicherheitsstandards für die Informationssicherheit in Kommunikationsnetzen und -diensten

Neben der Standardisierung, die durch die technische Kompatibilität innerhalb von Kommunikationssystemen notwendig wird, kann die Setzung von Standards besonders nach der Aufgabe der staatlichen Monopolgesellschaften im Telekommunikationsmarkt zur Reduzierung von Wohlfahrtsverlusten beitragen. Deren Ursachen liegen, wie bereits gezeigt, in den Informationsasymmetrien und in den Externalitäten im Bereich der Informationssicherheit begründet.[620]

Durch die Setzung verbindlicher Mindestssicherheitsstandards für Informationssicherheitssysteme in Kommunikationsnetzen und -diensten, die sich vor allem auf die von den Teilnehmern nicht oder nur unzureichend antizipierbaren Sicherheitseigenschaften beziehen sollten, wird das Qualitätsspektrum eingeschränkt und damit die asymmetrische Informationsverteilung zuungunsten der Nachfrager abgebaut.[621] Des weiteren können die negativen Externalitäten, die durch die Verletzung der Informationssicherheit verursacht werden, durch Sicherheitsstandards, die über dem von den Teilnehmern präferierten Informationssicherheitsniveau liegen, reduziert werden.[622] Die Durchsetzung von Mindestanforderungen hinsichtlich der Installation von Informationssicherheitssystemen in Kommunikationsnetzen und -diensten erreicht also sowohl den Abbau der vorgestellten Informationsasymmetrien als auch der negativen Externalitäten. Schließlich kann die Vorgabe von Mindestsicherheitsstandards für die Informationssicherheit dadurch gerechtfertigt werden, daß bei Schadensfällen immer auch immaterielle Nutzeneinbußen zu erwarten sind, die durch finanzielle Kompensationen im Rahmen eines Haftungssystems nicht oder nur unzureichend entschädigt werden können.[623]

Eine stärkere Berücksichtigung von Aspekten der Informationssicherheit im Standardisierungsprozeß kann zum einen durch eine entsprechende Besetzung der Normierungsgremien und zum anderen durch die Regulierung der Standardisie-

---

620 Vgl. Knorr (1993), S. 90f, zur Diskussion dieser Möglichkeit, welche aber die bekannten Ineffizienzen eines Monopols mitsichbringt. David & Steinmueller (1994), S. 222, argumentieren, daß durch die Deregulierung der staatlichen Monopole auch der allgemeine Standardisierungsbedarf steigt.

621 Knorr (1993), S. 44f, spricht in einem allgemeineren Zusammenhang von Transaktionskostenersparnissen.

622 Entsprechend Abb. 21 S. 221 ist ein Mindestsicherheitsstandard dann wohlfahrtssteigernd, wenn er jeweils zu Informationssicherheitsmaßnahmen führt, die mindestens über r^*_{privat} und höchstens in Höhe von r^*_{sozial} liegen.

623 Vgl. auch die Argumentation des System Security Study Committee u. a. (1991), S. 166f.

rungsaktivitäten in bezug auf die Erfordernisse der Informationssicherheit erreicht werden. Die Standardisierungsergebnisse sollten dann ihren Niederschlag in der Zulassungspraxis der Regulierungsbehörde finden. Die konkrete Ausgestaltung dieser Strategien wird im folgenden dargestellt, bevor abschließend die Setzung von Mindestanforderungen an die Informationssicherheit in Kommunikationssystemen nach allokativen, distributiven und administrativen Gesichtspunkten beurteilt wird.[624]

2.7.5.4 Die Regulierung der Zusammensetzung der Standardisierungsinstitutionen von Kommunikationsnetzen und -diensten

Aufgrund der voranschreitenden Liberalisierung der Telekommunikationsmärkte hat sich auch die Zusammensetzung der Normierungsgremien in die Richtung geändert, daß zu den staatlichen Anbietern von Kommunikationsnetzen und -diensten auch private Telekommunikationsunternehmen hinzugekommen sind.[625] Durch das Zurückdrängen und die Privatisierung der staatlichen Monopolgesellschaften werden die Standardisierungsinstitutionen in immer stärkerem Maße von den Interessen der privaten Anbieter dominiert, so daß die Interessen der Kommunikationsteilnehmer auch im Bereich der Informationssicherheit in den Hintergrund treten.

Deshalb sollten diese Institutionen verstärkt mit Vertretern von Verbänden besetzt werden[626], welche die Interessen von Kommunikationsteilnehmern organisieren.[627] Aufgrund der generellen Organisationsprobleme von Verbraucherverbänden[628], die durch die internationale Dimension des Problems noch verschärft wird, reicht die Ausstattung der Kommunikationsteilnehmervertreter mit Beteiligungs- und Stimmrecht in Standardisierungsinstitutionen nicht aus. Vor allem den Organisationen der nicht-kommerziellen Nutzer müssen sowohl finanzielle Mittel als auch technisches

---

624 Es wird nicht auf die Durchsetzung spezifischer technischer Eigenschaften von Informationssicherheitsmechanismen in Kommunikationssystemen eingegangen.

625 Dies hängt auch mit der zunehmenden Integration von Telekommunikations- und Informationstechnik zusammen. Vgl. zu Reformvorschlägen, die aus dieser Entwicklung folgen müssen, Knorr (1993), S. 162ff. Die komplexen Probleme, die mit der internationalen Dimension der Standardisierung und Regulierung zusammenhängen, werden im Rahmen dieser Arbeit nicht näher beleuchtet.

626 Dies fordern auch Kubicek (1991), S. 56, und Müller (1994a), S. 4. Knorr (1993), S. 140 FN 103, sieht dies als ein Grund für suboptimale Standards an.

627 Es gibt bereits Organisationen, die die Interessen kommerzieller und privater Telekommunikationsanwender repräsentieren. Vgl. Macpherson (1990), S. 285-301.

628 Vgl. zu einer speziellen ökonomischen Analyse dieser Problematik in Standardisierungsprozessen Foray (1994), S. 274-281.

Know-how bereitgestellt werden[629], damit sie eine effektive Vertretung ihrer Interessen durchsetzen können, weil ihre Arbeit sehr stark durch die Trittbrettfahreranreize der privaten Teilnehmer beeinträchtigt wird. Einzelne Privatteilnehmer haben sowohl geringe Grenznutzen als auch hohe Grenzkosten durch die Beteiligung am Standardisierungsprozeß, so daß sie ihre Interessen nicht wahrnehmen werden. Dagegen haben kommerzielle Teilnehmer durch ihre begrenzte Anzahl geringere Organisationskosten, und sie können durch die Expansion des Telekommunikationssektors nach erfolgreichen Standardisierungsbemühungen höhere Gewinne erwarten.

Des weiteren sollten die Interessen derjenigen gesellschaftlichen Gruppen, die besonders von den negativen Externalitäten der Verletzungen der Informationssicherheit tangiert werden, in den Standardisierungsgremien vertreten sein. Hinsichtlich des Schutzes der Übermittlung persönlicher Daten in Kommunikationssystemen sollten den nationalen Datenschutzbehörden ein Mitspracherecht eingeräumt werden.[630] Weiterhin legitimiert die zunehmende Beherrschung des Arbeitslebens durch die Kommunikations- und Informationstechnik auch eine Einflußnahme der Gewerkschaften[631] und der Arbeitgeberverbände. Schließlich macht die Verbreitung der Telemedizin im Gesundheitswesen eine Repräsentation der davon betroffenen Gruppen - Krankenhäuser, Ärzte und Patienten - in den Institutionen, die über die Standardisierung der dafür in Frage kommenden Kommunikationssysteme entscheiden, notwendig.[632]

Insgesamt bleibt festzuhalten, daß in den Standardisierungsinstitutionen zukünftig neben den Anbietern von Kommunikationsnetzen und -diensten auch Vertreter der jeweiligen Teilnehmer und der durch die entsprechenden Kommunikationsvorgänge indirekt Betroffenen beteiligt werden sollten, damit bereits vor Installierung der Kommunikationssysteme sowohl ein Abbau von Informationsasymmetrien als auch eine Internalisierung externer Effekte erreicht werden kann.

---

629 David & Greenstein (1990), S. 25, betonen, daß in Standardisierungsinstitutionen besonders die Verbrauchervertreter der technisch anspruchsvollen Auseinandersetzung nur bedingt folgen können.

630 Vgl. u. a. Höller (1993), S. 45.

631 Vgl. zu den ersten Gewerkschaftsinitiativen in diesem Bereich ebenda, S. 46.

632 Vgl. zu den neusten Entwicklungen der Telemedizin Adamik (1995).

2.7.5.5 Die Regulierung des Standardisierungsverfahrens durch die Vorgabe von Mindestsicherheitsstandards

Obwohl durch die Regulierung der Besetzung von Standardisierungsinstitutionen die Interessen von Kommunikationsteilnehmern und indirekt betroffenen Gruppen stärker berücksichtigt werden, ist damit nicht unbedingt sichergestellt, daß sich ein Niveau an Informationssicherheit herausbildet, welches dem gesellschaftlichen Optimum nahekommt. Deshalb sollte als komplementäre Maßnahme den Mitgliedern des Standardisierungskomitees vor dem eigentlichen Standardisierungsprozeß gewisse Mindestanforderungen für die Informationssicherheit von einer Regulierungsbehörde vorgegeben werden, denen der zu entwickelnde Standard zu entsprechen hat. Ferner werden durch die Besetzung von Standardisierungsgremien mit verschiedenen Organisationen die Interessenstrukturen heterogener. Die Folge davon ist eine Verzögerung der Standardisierungsprozesses aufgrund der schwierigeren Konsensfindung.[633] Die Vorgabe von Mindestanforderungen kann deshalb auch dazu beitragen, den Verlust der durch die Berücksichtigung der verschiedenen Interessen gewonnenen Wohlfahrtsgewinne aufgrund langsamer oder gar unmöglich gewordener Standardisierungsverfahren zu vermeiden.

Für die Bundesrepublik Deutschland bietet es sich an, daß diese Regulierungsinstitution mit derjenigen identisch ist, die nach den Plänen des Bundesministeriums für Post und Telekommunikation (BMPT) über die Zulassung der Betreiber von Kommunikationsnetzen und -diensten bestimmen soll.[634] Denn eine Lizenzvergabe soll nur bei Erfüllung bestimmter vorher festgelegter und veröffentlichter Grundanforderungen, worunter implizit auch die Eigenschaften der Informationssicherheit fallen, erfolgen.[635] Neben den Synergieeffekten, die durch die Setzung von Mindestsicherheitsstandards und deren Überprüfung bei der Lizenzvergabe an potentielle Anbieter in einer einzigen Regulierungsbehörde verursacht werden[636], soll die Vorgabe von Mindestsicherheitsanforderungen auch den eigentlichen Standardisierungsprozeß beschleunigen, weil ex ante eine Beschränkung des Standardisie-

---

633 Vgl. allgemein zum Trade-off zwischen der Standardisierungsgeschwindigkeit und der Integration verschiedener Interessengruppen Foray (1994), S. 286ff.

634 Grundsätzlich kann die Regulierung der Informationssicherheit in Kommunikationssystemen auch durch das BSI durchgeführt werden, indem dessen Kompetenzen erweitert werden. Außerdem kann auf europäischer Ebene auf die bereits existierenden Institutionen SAGE und STAG zurückgegriffen werden.

635 Vgl. BMPT (1995), S. 7f.

636 Die Mindestsicherheitsstandards können z. B. bereits so definiert werden, daß die Kontrollkosten ihrer Überwachung gering ausfallen.

rungsergebnisses vorgenommen wird.[637] Trotzdem erlaubt dieses Verfahren eine Vielfalt an Kommunikationsstandards bzw. -systemen, daß sich trotz unvollständiger Standardisierung einen Meta-Standard analog zum OSI-Referenzmodell ausbilden kann, der eine Verbindung der verschiedenen Kommunikationssysteme zu geringen und kalkulierbaren Kosten ermöglicht.[638]

Die Mindestanforderungen an sich sollten nicht als Objektnormen sondern als Ergebnisnormen formuliert werden[639], die z. B. an die von der Europäischen Kommission entwickelten „Information Technology Security Evaluation Criteria" (ITSEC) angelehnt werden könnten. In diesem Fall müssen die Informationssicherheitsmechanismen der verschiedenen Kommunikationssysteme lediglich bestimmte Leistungseigenschaften und keine konkreten technischen Konstruktionsnormen erfüllen.

Eine hohe Informationssicherheit kann aber nur dann realisiert werden, wenn die vorhandenen Informationssicherheitssysteme von den Mitarbeitern der Anbieter sorgfältig und nicht mißbräuchlich eingesetzt werden. Deshalb sollten die technischen Vorgaben durch personelle Auflagen flankiert werden, damit eine effiziente Kontrolle der Anforderungen möglich wird.[640]

2.7.5.6 Personelle Auflagen für die Betreiber von Kommunikationsnetzen und -diensten

Da §36 BDSG, der die Bestellung eines Beauftragten für den Datenschutz in Unternehmen, die personenbezogene Daten verarbeiten, verlangt, auch die Betreiber von Kommunikationsnetzen und -diensten betrifft, sollten in diesen Fällen die speziellen Datenschutzaufgaben nach §37 BDSG um die allgemeinen Aspekte der

---

637 Bei diesem Verfahren bleibt jedoch offen, nach welchen Kriterien die Mindestanforderungen ermittelt werden und in welchem Zusammenhang die Standardisierungs- mit den aktuellen Forschungsaktivitäten stehen sollten. Gerade hinsichtlich der Kriterien für die Informationssicherheit, die Kommunikationssysteme erfüllen sollten, existieren starke Divergenzen. Vgl. Rannenberg (1994).

638 Vgl. zum Konzept des Meta-Standards Foray (1994), S. 289f. Die Herausbildung eines einheitlichen Standards steht also nicht im Widerspruch zu der Modellannahme von Kapitel 2.4, die eine Vielfalt von Netzen und Diensten zuläßt. Durch einen Meta-Standard wird lediglich der Aufbau von Verbindungen zwischen verschiedenen Systemen erleichtert.

639 Vgl. David & Greenstein (1990), S. 30.

640 Die zur Sicherung der Informationssicherheit verwendeten Verschlüsselungstechniken sind nur dann effektiv, wenn mit den geheim zu haltenden Schlüsseln vertrauenswürdig umgegangen wird. Vgl. Garbe (1991), S. 117, und Wolfenstetter (1991), S. 124.

Informationssicherheit erweitert werden.[641] Damit ist auch eine Kompetenzerweiterung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz hin zur Kontrolle der Informationssicherheit verbunden.

Werden die negativen Externalitäten durch Verletzungen der Informationssicherheit als so schwerwiegend angesehen, daß sich dadurch ein direktes staatliches Intervenieren legitimieren läßt, bietet sich im Bereich der Verschlüsselungssysteme, die zur Gewährleistung der Informationssicherheit in Kommunikationssystemen beitragen, trotz der Integration von Übertragungs- und Informationssicherheitstechnik die Schaffung einer staatlichen Institution an. Alle Chiffriermethoden, die die Vertraulichkeit und Integrität der Kommunikationsinhalte sicherstellen sollen, können nur dann Informationssicherheit gewähren, wenn die öffentlichen Schlüssel der einzelnen Kommunikationsteilnehmer sorgfältig verwaltet werden.[642] Dafür kann der Staat eine Institution schaffen und mit Beamten besetzen, die für ein vertrauenswürdiges Schlüsselmanagement sorgen.[643] Der Grund für eine solche Maßnahme liegt darin, daß es sich bei Informationssicherheit um ein Vertrauensgut handelt, das nur realisiert werden kann, wenn die technisch vorhandenen Informationssicherheitssysteme nicht mißbräuchlich benutzt werden.

2.7.5.7 Eine Bewertung der Regulierung von Standardisierungsverfahren und Standardisierungsergebnissen

Im Gegensatz zum ungewissen Erfolg der Subventionierung von Informationssicherheitssystemen kann durch die simultane Regulierung der Standardisierungsverfahren und deren Ergebnisse mit hoher Zuverlässigkeit ein gewisser Mindeststandard bezüglich der Informationssicherheit in Kommunikationsnetzen und -diensten erreicht werden. Weiterhin werden durch die frühzeitige Berücksichtigung von Aspekten der Informationssicherheit im Prozeß der Standardentwicklung vor der Installation neuer Netze und der Markteinführung zusätzlicher Dienste Irreversibilitäten bei Hard- und Software vermieden.[644] Denn eine Nachrüstung bereits vor-

---

[641] Vgl. Roy (1995) zu den datenschutzrechtlichen Aspekten der Privatisierung der Deutschen Bundespost.

[642] Vgl. zur Schlüsselverwaltung bei asymmetrischen Verschlüsselungssystemen, Pfitzmann (1990), S. 26ff.

[643] Wolfenstetter (1991), S. 124, schlägt dafür einen sogenannten „Trust Center" vor. Leiberich (1995), S. 6, entwickelt Vorschläge, die auch die Bedürfnisse der inneren und äußeren Sicherheit mit berücksichtigen.

[644] Vgl. Knorr (1993), S. 112ff, zur allgemeinen Irreversibilitätsproblematik in der Telekommunikation, die jedoch durch die Digitalisierung an Bedeutung verliert.

handener Kommunikationssysteme mit zusätzlichen Informationssicherheitsmechanismen ist in vielen Fällen überhaupt nicht oder nur unter Aufwendung hoher Kosten möglich.

Weiterhin ist die Vorgabe von Mindeststandards hinsichtlich der Entwicklung einer gewissen Vielfalt von Kommunikationsnetzen und -diensten positiv zu bewerten. Da keine technischen, sondern lediglich Leistungseigenschaften verlangt werden, wird der Standardisierungsprozeß nicht zu sehr eingeengt, so daß sich unvollständig spezifizierte Standards herausbilden können, die eine Vielfalt von Netzen und Diensten ermöglichen.

Kritisch ist gegen Mindestsicherheitsstandards einzuwenden, daß diese entsprechend der Ergebnisse aus Kapitel 2.6 für Kommunikationssysteme mit hohen Teilnehmerzahlen und starker Leistungsfähigkeit in ihren Anforderungen ansteigen sollten, so daß hinsichtlich der Qualitätsregulierung durch Mindestsicherheitsstandards erhebliche Informationsprobleme bestehen.[645] Ein einheitlicher Sicherheitsstandard für alle Kommunikationsdienste und Netze ist mit hohen Wohlfahrtsverlusten verbunden, wobei für netzübergreifende Verbindungen ein gewisser gemeinsamer Mindestlevel an Sicherheitseigenschaften angebracht ist[646], der eine zu starke Differenzierung unmöglich macht. Weiterhin existieren neben diesen Gesichtspunkten, die auf statische Wohlfahrtsverluste von Mindestsicherheitsstandards hindeuten, auch dynamische Allokationsineffizienzen. Die Vorgabe von Mindestsicherheitsstandards vor allem in Form von Objektnormen schränkt ex ante die möglichen Ergebnisse des Standardisierungsprozesses ein.

Da eine strikte Trennung zwischen Standardisierungs- und Forschungsaktivitäten, wie in Abschnitt 2.7.6 noch näher ausgeführt wird, nicht möglich ist, bedeutet dies unmittelbar auch eine Begrenzung der Forschungsaktivitäten. Dies kann besonders dann zur Herausbildung eines suboptimalen Standards führen, wenn der Formulierung der Mindestanforderungen keine umfassenden Forschungsaktivitäten vorausgehen.[647] Allerdings kann die Anbieterseite auch die Standardisierungsaktivitäten im Bereich der Informationssicherheit verzögern, indem auf unzureichende For-

---

645 Vgl. Bauer (1992), S. 106ff.

646 Dies wird auch im Eckpunkte-Papier über den künftigen Regulierungsrahmen des BMPT (1995), S. 11, gefordert.

647 Vgl. allgemein zur Interdependenz von Standardsetzung und Innovationstätigkeit David & Steinmueller (1994), S. 238ff. Knieps (1994), S. 18f, lehnt sowohl eine staatliche Standardsetzung als auch eine Regulierung von Standardisierungsinstitutionen in einem Kontext ohne Externalitäten und Informationsasymmetrien ab.

schungserkenntnisse verwiesen wird. Diese Verzögerungsstrategie ist vor allem bei Umweltstandards zu beobachten und kann letztendlich auch den Fortschritt der Informationssicherheit in offenen Kommunikationssystemen behindern.

Der Standardisierungsprozeß und die sich daran anschließende Einführung neuer Kommunikationsnetze und -dienste werden durch die vorgegebene Besetzung der Standardisierungsinstitutionen mit den Vertretern der von Verletzungen der Informationssicherheit betroffenen Gruppen verlangsamt werden. Diese Verzögerung kann als Preis für die Entwicklung von gesellschaftlich optimalen Kommunikationsstandards angesehen werden, die nicht durch die Interessen der Angebotsseite dominiert werden.

Unter Verteilungsgesichtspunkten ist die Festsetzung verbindlicher Mindestsicherheitsstandards gerechtfertigt, weil die Kommunikationsteilnehmer die daraus folgenden Kosten zu tragen haben und damit das Verursacherprinzip Geltung erlangt, indem die für die negativen Externalitäten Verantwortlichen auch für die Internalisierungskosten herangezogen werden.[648] Verteilungsungerechtigkeiten zwischen den Kommunikationsteilnehmern könnten insofern auftauchen, als diejenigen mit geringem Schadenpotential oder mit einer risikoneutralen Einstellung einen niedrigen Sicherheitsstandard vorziehen und durch die Mindestsicherheitsstandards übermäßig belastet werden. Falls Mindestvorgaben entsprechend der Netzeigenschaften Teilnehmerzahl n^* und Integrationsgrad I^* vorgegeben werden und sich in den einzelnen Netzen oder Diensten homogene Teilnehmer zusammenfinden, dann werden die Verteilungsungerechtigkeiten nicht sehr gravierend sein.

Die unmittelbaren Kosten der Regulierung durch Mindestsicherheitsstandards setzen sich aus den Aufwendungen, die der Formulierung von Mindestanforderungen vorausgehen, den Zulassungs- bzw. Überprüfungskosten der Regulierungsbehörde und den Personalkosten eines staatlichen Schlüsselmanagements zusammen. Im Vergleich zu den anderen Strategien ist die Entwicklung, Durchsetzung und Kontrolle von Mindestsicherheitsstandards sicherlich die Lösung, bei der die höchsten direkten Kosten anfallen, denen jedoch die unmittelbaren Vorteile einer sichereren Allokationsverbesserung gegenübergestellt werden müssen.

---

648 Das Verursacherprinzip wird insofern durchbrochen, als daß die Kosten der Regulierungsbehörden durch die Gemeinschaft getragen werden. Deshalb sollte die Finanzierung der Teilnehmerinteressenvertretung in den Standardisierungsinstitutionen nicht aus allgemeinen Steuereinnahmen, sondern mit einer speziellen Steuer auf Telekommunikationsleistungen getragen werden.

2.7.6 Staatliche Forschungsförderung von Informationssicherheitssystemen in Kommunikationsnetzen und -diensten

2.7.6.1 Die fehlende Legitimation einer staatlichen Bereitstellung von Informationssicherheit in Kommunikationsnetzen und -diensten

Nach der direkten Regulierung der Anbieter von Kommunikationsnetzen und -diensten durch Mindestsicherheitsstandards gilt es schließlich noch als letzte Möglichkeit zur Sicherstellung eines optimalen Informationssicherheitsniveaus, die staatliche Gewährleistung von Informationssicherheit in Kommunikationssystemen in Analogie zu Bereitstellung äußerer und innerer Sicherheit zu analysieren.

Unter theoretischen Gesichtspunkten darf eine staatliche Bereitstellung von Informationssicherheit in Kommunikationssystemen nicht erfolgen, weil sowohl das Ausschlußprinzip in Kommunikationsnetzen und -diensten von den jeweiligen Betreibern durchgesetzt werden kann als auch mit zunehmender Teilnehmerzahl Überfüllungserscheinungen und damit Rivalitäten bei der Nutzung der Informationssicherheitssysteme zu beobachten sind. Überdies existieren unauflösliche technische Interdependenzen zwischen der Kommunikationstechnik und den Informationssicherheitsmechanismen. Deshalb wäre eine staatliche Bereitstellung von Informationssicherheit in Kommunikationssystemen mit einer Überführung aller privaten Telekommunikationsunternehmen in staatliche Betriebe verbunden, was angesichts der weltweiten Liberalisierungstendenzen und den damit verbundenen Kosten für den Staatshaushalt politisch nicht durchzusetzen ist.

2.7.6.2 Die Legitimation und Ausgestaltung staatlicher Forschungsförderung der Informationssicherheit in Kommunikationsnetzen und -diensten

Die staatliche Förderung von Grundlagenforschung wird im allgemeinen dadurch begründet, daß die gewonnenen Erkenntnisse die Eigenschaften öffentlicher Güter haben. Zum einen ist das Ausschlußprinzip nicht durchzusetzen, weil die Forschungsergebnisse spätestens ab ihrer kommerziellen Verwertung für alle zugänglich sind. Zum anderen ist die Verbreitung der Erkenntnisse mit sehr geringen Kosten verbunden, so daß ein Schutz durch Patente oder hohe Lizenzgebühren nicht

wohlfahrtsoptimal ist.[649] Ferner ist bei der Setzung von Mindestsicherheitsstandards schon unmittelbar deutlich geworden, daß dem Einsatz dieses Instrumentes eine intensive Forschungstätigkeit vorausgehen muß, damit sich nicht suboptimale Kommunikationsstandards herausbilden. Deshalb sollte die Grundlagenforschung im Bereich der Informationssicherheit entweder finanziell unterstützt oder unmittelbar von staatlichen Stellen betrieben werden.

Auf nationaler Ebene hat die Bundesrepublik Deutschland im BSI bereits eine staatliche Forschungseinrichtung. Es ist für die Untersuchung von Sicherheitsrisiken bei der Anwendung von Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit der Informationstechnik, soweit dies die Erfüllung von Aufgaben des Bundes erfordert, zuständig.[650] Durch eine Streichung letzterer Einschränkung und eine Kompetenzerweiterung auf den allgemeinen Bereich der Kommunikationssysteme kann das BSI Grundlagenforschung leisten. Weiterhin muß die im Rahmen der Liberalisierung des Telekommunikationsmarktes zu schaffende Regulierungsbehörde auch Forschungsaufgaben wahrnehmen, die von der privatisierten Deutschen Telekom AG nicht mehr wahrgenommen werden.[651]

Die Darstellung der europäischen Normungsgremien SAGE und STAG, deren Aktivitäten vor allem durch den EG-Haushalt finanziert werden, hat bereits gezeigt, daß eine klare Trennung zwischen Forschungs- und Standardisierungsaktivitäten nicht möglich ist. Um Fortschritte in der Forschung und Standardisierung von Informationssicherheitssystemen zu erreichen, ist ein Koordination von Forschungs- und Standardisierungsinstitutionen notwendig. Um eine suboptimale Standardsetzung bei Kommunikationssystemen durch staatliche Vorgaben zu vermeiden, muß also eine fundierte Forschungstätigkeit vorausgehen. Neben der Legitimation von Grundlagenforschung über die Eigenschaften eines öffentlichen Gutes rechtfertigen Synergieeffekte zwischen staatlichen Regulierungsaktivitäten und neusten Forschungserkenntnissen staatliche Forschungsanstrengungen im Feld der Informationssicherheit von Kommunikationssystemen. Obwohl diese Forschung auch die Betreiber von Kommunikationsnetzen und Diensten durchführen könnten, sollte der Staat eine unabhängige Forschungseinrichtung finanzieren, damit die Richtung

---

[649] Vgl. u. a. Hirshleifer & Riley (1992), S. 259ff. Außerdem existiert zumindest theoretisch die Tendenz zu privaten Überinvestitionen in Forschungsaktivitäten, die durch gleichzeitiges Forschen nach denselben neuen Erkenntnissen verursacht wird.

[650] Vgl. BGBl. S. 2834 vom 17. 12. 1990 §3 BSI-Gesetz Absatz 1 Nr. 1.

[651] Vgl. Wolfenstetter (1991) zu den Forschungsaktivitäten der ehemaligen DBP Telekom.

der Forschungsaktivitäten nicht von angebotsseitigen Interessen dominiert wird. Für eine solche Aufgabe sind auf nationaler Ebene das BSI und auf europäischer Ebene die Forschungseinrichtungen der ETSI durchaus befähigt.[652]

2.7.6.4 Die Bewertung der staatlichen Forschungsförderung

Staatliche Forschungsaktivitäten im Bereich der Informationssicherheit von Kommunikationssystemen können sicherlich zum Fortschritt in diesem Bereich beitragen und damit auch intertemporale Externalitäten vermeiden, die heutige Standardisierungsinstitutionen durch die Implementierung suboptimaler Kommunikations- und Sicherheitsstandards für spätere Nutzergenerationen hervorrufen können.[653]

Inwieweit es sich bei Erkenntnissen der Grundlagenforschung im Bereich der Informationssicherheits- und der damit verbundenen Kommunikationstechnik um ein öffentliches Gut handelt, ist nicht eindeutig abzugrenzen. Denn die Forschungsaktivitäten in diesen Bereichen haben in vielen Fällen einen unmittelbaren Bezug zu konkreten Anwendungen. Damit haben die privaten Anbieter von Kommunikationsanlagen und -systemen ausreichende Anreize zu eigenen Forschungsanstrengungen. Da aber hierbei Aspekte der Informationssicherheit eher vernachlässigt werden, können staatliche Forschungsaktivitäten zum Abbau der Allokationsineffizienzen beitragen, die durch ein suboptimales Niveau an Informationssicherheit in Kommunikationssystemen verursacht werden.

Von einer Verbesserung der Standardsetzung aufgrund staatlicher Forschungserkenntnisse haben zunächst die Kommunikationsteilnehmer selbst einen Vorteil. Indirekt sind aber auch die übrigen Gesellschaftsmitglieder Nutznießer, so daß die negativen Verteilungseffekte innerhalb der Gesellschaft begrenzt sind. Die Globalisierung der Kommmunikationssysteme verlangt aber eine internationale Koordination nationaler Forschungsaktivitäten, ansonsten kann es zu einem kostenlosen Transfer der Erkenntnisse nationaler Forschungsanstrengungen in Form der Standardsetzung kommen. Wenn nationale Präferenzunterschiede hinsichtlich der Informationssicherheit in Kommunikationsnetzen existieren, dann führt das Einneh-

---

652 Es ist aber durchaus eine Kompetenzerweiterung des Bundesamtes für Post und Telekommunikation vorstellbar, die analog zum Umweltbundesamt auch eine wissenschaftliche Unterstützung der neu zu gründenden Regulierungsinstitution beinhalten kann.

653 Vgl. dazu David & Greenstein (1990), S. 7. Im Bereich der Interdependenzen zwischen Standardsetzung und Innovationen wird immer noch ein theoretischer Forschungsbedarf konstatiert. Vgl. ebenda S. 34 und David & Steinmueller (1994), S. 239.

men einer Vorreiterrolle, indem der nationale Standard weltweite Akzeptanz erlangt, zu einer Internaliserung negativer Externalitäten, die durch die Interdependenzen zwischen Kommunikationssystemen mit unterschiedlichem Sicherheitsniveau hervorgerufen werden.[654]

Die fiskalischen Kosten einer staatlichen Forschungsförderung belaufen sich auf die Ausstattung einer Forschungseinrichtung mit Sach- und Personalmitteln.[655] Ein Begrenzung der Kosten kann durch die Ausführung externer Forschungsaufträge erreicht werden, die SAGE unter Nutzung vorhandener Kapazitäten gegen eine finanzielle Entschädigung durchführt.

2.7.7 Fazit: Eine zusammenfassende Politikempfehlung

Zum Abschluß der Darstellung und Bewertung der verschiedenen Instrumente wird keine Zusammenfassung der gewonnenen Erkenntnisse, sondern eine Analyse der Relationen zwischen den verschiedenen Politikalternativen vorgenommen. Dazu gibt die Übersicht 13 zunächst einen Überblick über die vorgestellten Instrumente und ihre prinzipielle Eignung hinsichtlich des Abbaus von Informationsasymmetrien und Externalitäten.

Ursachen / Instrumente	Informationsasymmetrien	Externalitäten
Informationspolitik	geeignet	weniger geeignet
Gefährdungshaftung	geeignet	geeignet
Subventionen	weniger geeignet	geeignet
Mindestsicherheits-standards	geeignet	geeignet
Forschungsförderung	weniger geeignet	geeignet

Übersicht 13: Ursachen von Allokationsineffizienzen und die Eignung der vorgestellten Instrumente

654 Vgl. dazu auch die Ausführungen in Abschnitt 2.6.3.1.

655 Vgl. z. B. zum Gesamthaushalt des BSI Fußnote 551auf S. 229.

Grundsätzlich sind lediglich das Haftungsrecht und die Regulierung dazu geeignet, sowohl die Informationsasymmetrien als auch die negativen Externalitäten hinsichtlich der Informationssicherheit von Kommunikationssystemen abzubauen. Jedoch kann die staatliche Informationspolitik sowohl zum Haftungsrecht als auch zur Regulierung komplementäre Aufgaben zum Abbau von Informationsasymmetrien übernehmen. Dasselbe gilt für die Subventionslösungen, welche die Netz- und Dienstebetreiber von den finanziellen Folgekosten des vorgeschlagenen Informationssicherheitshaftungsgesetzes und der staatlichen Regulierungsmaßnahmen entlasten können.

Die staatliche Forschungsförderung kann mit ihren Erkenntnissen über den Problembereich der Informationssicherheit sowohl bei der Durchsetzung des Haftungsrechtes hilfreiche Dienste leisten als auch, wie ausgeführt, bei der Formulierung von Mindestsicherheitsstandards die Entwicklung suboptimaler Standards vermeiden helfen. Darüber hinaus muß sich eine wirksame staatliche Informationspolitik auch auf die aktuellen Forschungserkenntnisse berufen, die durch eine unabhängige staatliche Forschungsinstitution wie dem BSI generiert werden können. Insgesamt bleibt also festzuhalten, daß es sich bei den vorgestellten Instrumenten um keine Substitute, sondern um Komplemente handelt, und damit ein gleichzeitiger Einsatz zur Vermeidung volkswirtschaftlicher Wohlfahrtsverluste gerechtfertigt ist.

Schließlich gilt es noch zu zeigen, daß auch zwischen dem Haftungsrecht und der Regulierung keine substitutive, sondern eine komplementäre Beziehung besteht.[656] Die Vorteile der Gefährdungshaftung liegen vor allem in der verwaltungskostengünstigen Setzung einer Präventionsanreizstruktur für die Betreiber von Kommunikationsnetzen und -diensten, die zu einem gesellschaftlich effizienten Informationssicherheitsniveau führen kann. Beeinträchtigungen der Allokationseffizienz ergeben sich zum einen dadurch, daß aufgrund der Komplexität von Kommunikationssystemen und der schwierigen Verifizierbarkeit von Verletzungen der Informationssicherheit den Netz- und Dienstebetreibern in vielen Fällen keine Schuld nachgewiesen werden kann. Zum anderen handelt es sich bei Verletzungen der Informationssicherheit oft um Vorgänge mit immateriellen Schadenskomponenten für die keine oder nur eine begrenzte monetäre Kompensation angesetzt wird.[657] Diese

---

[656] Vgl. allgemein dazu Shavell (1984), (1984a), Skogh (1989) und Kolstad, Ulen und Johnson (1990).

[657] Als weiterer theoretischer Grund wird von Shavell (1984), S. 365, die Zahlungsunfähigkeit bei Schadensfällen mit katastrophalem Ausmaß angegeben, welche jedoch bei multinationalen Netz- und Dienstebetreibern nicht droht.

Aspekte verleiten die Betreiber von Kommunikationsnetzen und -diensten trotz Gefährdungshaftung zu einem suboptimalen Präventionsniveau hinsichtlich der Informationssicherheitsmaßnahmen. Durch die Setzung von Mindestsicherheitsstandards kann diese Schwäche der Gefährdungshaftung ausgeglichen werden. Damit ist offensichtlich geworden, daß es sich bei Gefährdungshaftung und gesetzlichen Mindestsicherheitsstandards nicht um substitutive, sondern um komplementäre Lösungsstrategien handelt.

2.8 Zusammenfassung und Ausblick

Dieses abschließende Kapitel faßt die wesentlichen theoretischen Erkenntnisse und die daraus folgenden wirtschaftspolitischen Implikationen kurz zusammen. Im Anschluß daran werden jeweils noch offengebliebene Problemstellungen für zukünftige Forschungstätigkeiten aufgezeigt, von denen im Rahmen dieser Arbeit abstrahiert wurde.

Die theoretische Effizienzanalyse in Kapitel 2.5 zeigt, daß für ein optimales Ausmaß an Informationssicherheit in offenen Kommunikationsnetzen aufgrund des Clubgutcharakters der Sicherheitssysteme in teilnehmerstärkeren Kommunikationssystemen auch pro Kommunikationsteilnehmer die Anstrengungen im Bereich der Informationssicherheit zunehmen müssen. Für Kommunikationssysteme mit höheren Übertragungskapazitäten kann aus den statischen Effizienzüberlegungen kein eindeutiger Zusammenhang zum Umfang der zu ergreifenden Informationssicherheitsmaßnahmen hergestellt werden. Mit zunehmender Komplexität und Kapazität der Kommunikationssysteme wird jedoch das Volumen an transportierten Informationen vor allem auf den zukünftigen Datenautobahnen immens ansteigen. Daher müssen unter Berücksichtigung eines kostensparenden technischen Fortschritts in der Informationssicherheitstechnik auch dementsprechend verstärkt Sicherheitsmaßnahmen ergriffen werden. Ferner ist unter Verwendung der Erwartungsnutzentheorie auch deutlich geworden, daß potentielle Verletzungen immaterieller Werte - wie z. B. der Privatsphäre - im Vergleich zu materiellen Verlusten einen verstärkten Einsatz von Informationssicherheitsmaßnahmen erfordern.

Die ökonomische Analyse hat Informationssicherheitsmaßnahmen von seiten der Teilnehmer nicht berücksichtigt, sondern lediglich dem Kommunikationssystem immanente Sicherheitsmechanismen unterstellt. Deshalb kann es für zukünftige Arbeiten in Analogie zu den bereits untersuchten Interdependenzen zwischen privaten und öffentlichen Maßnahmen zur Herstellung der inneren Sicherheit interessant sein, auch in offenen Kommunikationssystemen teilnehmer- und netzspezifische Maßnahmen zur Informationssicherheit zu unterscheiden und Bedingungen für komplementäre oder substitutive Relationen zu bestimmen.

Weiterhin sind in Kapitel 2.5 für die Risiken der Informationssicherheit in offenen Kommunikationssystemen die Versicherungsnachfrage theoretisch bestimmt und das aktuelle Versicherungsangebot beschrieben worden. Wie oben dargestellt, können Verletzungen der Informationssicherheit auch immaterielle Verluste verursachen. Aus dem Erwartungsnutzenkalkül kann bei immateriellen Risiken keine po-

sitive Versicherungsnachfrage abgeleitet werden. Ferner verhindern Informationsasymmetrien zuungunsten der privaten Versicherer, daß für viele Risiken der Informationssicherheit kein Versicherungsschutz angeboten wird. Es bleibt deshalb die Frage zu klären, ob nicht meritorische Gesichtspunkte und steigende negative Externalitäten durch die Risiken der zukünftigen Informations- und Kommunikationsgesellschaft eine gesetzliche Versicherungslösung legitimieren können. Mit Beginn der Industrialisierung wurden schließlich auch zahlreiche gesetzliche Versicherungen eingeführt, die den Arbeitemehmern einen Schutz gegen die zahlreichen neuen Risiken industrieller Produktion bieten sollten. Unmittelbar daran schließt sich das noch völlig ungeklärte Problem der Ausgestaltung einer solchen Versicherungslösung an.

Wie schon im Rahmen der Versicherungsproblematik angesprochen, gibt es ökonomische Gründe dafür, daß die Betreiber offener Kommunikationsnetze und -dienste ineffiziente bzw. suboptimale Anstrengungen hinsichtlich der Installation von Informationssicherheitssystemen unternehmen werden. In Kapitel 2.6 werden sowohl asymmetrische Informationsverteilungen hinsichtlich Schadenswahrscheinlichkeiten und Wirksamkeit von Informationssicherungsmechanismen zwischen der Anbieter- und der Teilnehmerseite als auch negative Externalitäten solcher Schadensfälle in Kommunikationssystemen als Ursachen für Allokationsineffizienzen identifiziert, die ein staatliches Eingreifen rechtfertigen können.

Ob diese Wohlfahrtsverluste durch veränderte Wettbewerbsbedingungen an Bedeutung gewinnen oder verlieren, wurde bei der Untersuchung ausgeklammert, weil eine statische Konkurrenzsituation auf dem Telekommunikationsmarkt unterstellt wurde. Inwieweit die Liberalisierung des Telekommunikationsbereichs in der Bundesrepublik Deutschland zu einer Herausbildung wettbewerblicher Marktstrukturen führen kann, wird sich erst in der Zukunft zeigen. Dennoch ist im Kontext der Informationssicherheit von Interesse, ob auch hier ein Anstieg des Wettbewerbsdrucks auf die Betreiber von Netzen und Diensten zumindest einen Abbau der asymmetrischen Informationsverteilung zuungunsten der Teilnehmer und damit ein effizienteres Niveau an Informationssicherheit herbeiführen kann. Es stellt sich hier generell die Frage, welche Preis-Leistungsverhältnisse ein stark wettbewerbsorientierter Kommunikationsdienstemarkt hervorbringt, wenn gleichzeitig die Situation bei den Netzanbietern schon aus technischen Gründen eher oligopolistische Strukturen aufweisen wird.

Anschließend wurden in Kapitel 2.7 staatliche Instrumente vorgestellt, die eine Verbesserung der Informationssicherheit in offenen Kommunikationssystemen versprechen. Neben staatlicher Informationspolitik, mit der in der Bundesrepublik Deutschland in weiten Teilen das Bundesamt für Sicherheit in der Informationstechnik betraut ist, erweist sich vor allem das Haftungsrecht als geeignet, die Informationsasymmetrien zwischen Anbietern und Nachfragern abzubauen und die für Teilnehmer und die übrige Gesellschaft negativen Externalitäten von Verletzungen der Informationssicherheit zu internalisieren. Unter der Annahme, daß die Kommunikationsteilnehmer keinen Einfluß auf die Informationssicherheit im Kommunikationssystem haben, erweist sich die Gefährdungshaftung als allokationseffiziente und dem Verursacherprinzip gerecht werdende Haftungsregel. Dies spiegelt sich auch in den Prinzipien des vorgeschlagenen Informationssicherheitshaftungsgesetzes wider. Wenn die Teilnehmer selbst das Informationssicherheitsniveau beeinflussen können und damit Moral Hazard möglich ist, ist eine tiefergehende Analyse erforderlich, die sicherlich differenziertere Ergebnisse hervorbringen wird.

Nach Aufgabe der staatlichen Netzmonopole im Telekommunikationssektor bietet sich zur Erreichung einer verbesserten Informationssicherheit in den offenen Kommunikationsnetzen auch eine direkte Subventionierung der privaten Netzbetreiber an. Die vorgeschlagenen Lösungen beziehen sich sowohl auf die Verbesserung der Informationssicherheit in schon bestehenden Kommunikationssystemen als auch auf die Unterstützung der Markteinführung neuer, mit zuverlässigeren Informationssicherheitssystemen ausgestatteten Netze und Dienste.

Schließlich wurden hinsichtlich des Standardisierungsprozesses von Kommunikationstechniken und -systemen zwei weitere Vorschläge unterbreitet. Zum einen müssen in den Standardisierungsgremien die Interessen der Teilnehmer und der indirekt betroffenen Bevölkerungsgruppen Berücksichtigung finden. Dies kann durch eine staatliche Regulierung der Zusammensetzung der Standardisierungsinstitutionen erreicht werden, wobei die Teilnehmervertreter sowohl finanziell unterstützt als auch mit den notwendigen technischen Kenntnissen versorgt werden müssen. Zum anderen kann der Gesetzgeber allgemeine Kriterien hinsichtlich der Informationssicherheit vorgeben, denen die Entwürfe der Standardisierungsgremien entsprechen müssen. Um suboptimale oder auch unrealisierbare Kommunikationsstandards zu vermeiden, ist es jedoch notwendig, daß diese Vorgaben die neuesten Forschungserkenntnisse enthalten. Die Arbeit einer staatlichen Regulierungsbehörde gewinnt an Effizienz, wenn der Staat selbst auf dem Gebiet der Informationssicherheit

forscht. Dafür ist schon das Bundesamt für Sicherheit in der Informationstechnik teilweise zuständig. Ein bereits in der Literatur geäußerter Forschungsbedarf besteht darin, die ambivalenten ökonomischen Implikationen der Interdependenzen zwischen Forschungs- und Standardisierungsaktivitäten zu untersuchen.

Ferner müssen alle vorgestellten staatlichen Instrumente auch auf ihre Eignung in einem globalen Telekommunikationsmarkt untersucht werden. In Analogie zur Problematik von Umweltstandards müssen die Internalisierungs- und Marktexpansionseffekte internationaler Informationssicherheitsstandards den Effizienzverlusten, die nationale Präferenzen für Informationssicherheit mitsichbringen, gegenübergestellt werden. Daran schließt sich unmittelbar die Frage an, ob ein hohes Niveau an Informationssicherheit in den nationalen Kommunikationssystemen einen Standortvorteil bedeuten und deshalb der Standortwettbewerb effiziente Lösungen hervorbringen kann.

Schließlich ist die strafrechtliche Bekämpfung der Computerkriminalität als mögliche Strategie zur Verbesserung der Informationssicherheit nicht in Erwägung gezogen worden. Eine ökonomische Analyse der Computerkriminalität kann sicherlich Aufschluß über die theoretische Effektivität dieser Strategie geben. In diesem Zusammenhang ist zu erwähnen, daß auch der aktuelle Konflikt über die ambivalente Rolle der Verschlüsselung in offenen Kommunikationssystemen neben dem rechtlichen Aspekt, der eine Abwägung der Rechtsgüter innerer Sicherheit und einer vor dem Staat geschützten Kommunikationsphäre erfordert, einer ökonomischen Effizienzanalyse unterzogen werden kann.

Literaturverzeichnis

Adamik, P. (1995): Ärzte können in Videokonferenz mit Kollegen über Therapie beraten, in: Das Handelsblatt 19. 4. 1995, S. 30.

Adams, M.(1987): Produkthaftung - Wohltat oder Plage - Eine ökonomische Analyse, in: Betriebsberater, Beilage 20/1987 zur Zeitschrift für Recht und Wirtschaft 31/1987, S. 1-24.

Adams, M. (1989): Warum kein Ersatz von Nichtvermögensschäden?, in: Allokationseffizienz in der Rechtsordnung hrsg. von Ott, C. und Schäfer H.-B., Berlin, Heidelberg u. a. 1989, S. 210-217.

Adams, W. J. und Yellen, J. L. (1976): Commodity Bundling and the Burden of Monopoly, in: Quarterly Journal of Economics, 90/1976, S. 475-498.

Allen, D (1988).: New telecommunications services: Network externalities and critical mass, in: Telecommunications Policy 12/1988, H. 3, S. 257-271.

Andel, N. (1992): Finanzwissenschaft, 3. Auflage, Tübingen 1992.

Antonelli, C.(Hrsg.) (1992): The Economics of Information Networks, Amsterdam 1992.

Arnott, R. und Stiglitz, J. E. (1986): Moral Hazard and Optimal Commodity Taxation, in: Journal of Public Economics 29/1986, S. 1-24.

Arnould, R. J. und H. Grabowski (1981): Auto safety regulation: an analysis of market failure, in: The Bell Journal of Economics, 12/1981, H. 1, S. 27-48.

Arrow, K. J. (1965): Aspects of the Theory of Risk Baring, Helsinki 1965.

Artle, R. und Averous, C.(1973): The telephone system as public good: static and dynamic aspects, in: The Bell Journal of Economics, 4/1973, H. 1, S. 89-100.

Asch, P. (1988): Consumer Safety Regulation, New York 1988.

Ault, E. B. (1988): CPCS'S Voluntary Standards: An Assessment and a Paradox - The Paradox of Voluntary standards for Consumer Products, in: The Frontier of Research in the Consumer Interest hrsg. von E. Scott Maynes und dem ACCI Research Committee, Columbia 1988, S. 77-107.

Bach, K. und Kubicek, H. (1992): Datenschutz bei Wettbewerbsdiensten, in: Computer und Recht 8/1992, H. 8, S. 482-492.

Barth, H. (1992): Moderne Telekommunikation: Netze, Dienste, Instrumente, Normen und praktischer Einsatz, München 1992.

Bauer, A. und Illinng, G. (1992): Transaktionskosten und das Coase-Theorem, in: Das Wirtschaftsstudium 21/1992, S. 933-936.

Bauer, B. (1992): Quality and Quality Regulation of Reserved Telecommunication Services, in: Telecommunication: New Signposts to Old Roads hrsg. von Klaver F. und Slaa, P. Amsterdam, Oxford u. a. 1992, S. 101-112.

Baumol, W. J., Panzar J. C. und Willig, R. D. (1988): Contestable Markets and the Theory of Industry Structure, San Diego, New York u. a. 1988.

Beales, H., Crasswell, R. und Salop, St. C. (1981): The Efficient Regulation of Consumer Information, in: Journal of Law and Economics 24/181, S. 491-539.

Behrendsen, H. P. (1992): Die bereichsspezifischen Datenschutzverordnungen für TK-Dienstleistungen, in: Computer und Recht 8/1992, H. 7, S. 422-430.

Berglas, E. (1976): On the Theory of Clubs, in: American Economic Review, 66/1976, H. 2, S. 116-121.

Besen, St. A. und Saloner G. (1989): The Economics of Telecommunications Standards, in: Changing the Rules: Technological Change, International Competition, and Regulation in Communications hrsg. von Crandall, R. W. und Flamm, K., Washington, D. C. 1989, S. 177-220.

Beutelspacher, A. (1987): Kryptologie, Braunschweig 1987.

Blankart, Ch. B. (1994): Öffentliche Finanzen in der Demokratie, 2. Auflage München 1994.

Blankart, Ch. B. und Pommerehne, W. W. (1985): Zwei Wege zur Privatisierung öffentlicher Dienstleistungen: Wettbewerb auf einem Markt und Wettbewerb um einen Markt - Eine kritische Beurteilung, in: Rationale Wirtschaftspolitik in komplexen Gesellschaften hrsg. von Milde, H. und Monissen, H. G., Stuttgart u. a. 1985, S. 431-442.

Blankart Ch. B. und Knieps, G. (1992): Netzökonomik, in: Jahrbuch für Neue Politische Ökonomie, 11. Band: Ökonomische Systeme und ihre Dynamik, hrsg. von Herder-Dorneich Ph., Schmidtchen D. u. a., Tübingen 1992, S. 73-87.

Bleymüller, J., Gehlert G. und Gülicher, H.: Statistik für Wirtschaftswissenschaftler, 7. Aufl. München 1991.

Blümel, W. , Pethig, R. und Hagen v. d. O. (1986): The Theory of Public Goods: A Survey on Recent Issues, in: Journal of Institutional and Theoretical Economics 142/1986, S. 241-309.

Borchers, D.(1995): Die Online-Welt, in: Die Zeit Nr. 6, 3. 2. 1995, S. 78.

Boyer, M. und Dionne, G. (1983): Variations in the probability and magnitude of loss: their impact on risk, in: Canadien Journal of Economics 16/1983, H. 3, S. 411-419.

Boyer, M. und Dionne, G. (1989): More on insurance, protection, and risk, in: Canadien Journal of Economics 22/1989, H. 1, S. 202-204.

Brandt, P. (1993): Mehr Sicherheit, mehr Geld - die Risikoanalyse, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 1993, H. 4, S. 56-58.

Brennan, T. J. und Kimmel, S. (1986): Joint Production and Monopoly Extension through Tying, in: Southern Economic Journal 53/1986/87, S. 490-501.

Briys, E. und Schlesinger, H. (1990): Risk Aversion and the Propensities for Self-Insurance and Self-Protection, in: Southern Economic Journal 57/1990, S. 458-467.

Buchanan, J. M. (1965): An Economic Theory of Clubs, in: Economica 32/1965, S. 1-14.

Buchanan, J. M.(1970): In Defense of Caveat Emptor, in: The University of Chicago Law Review, 38/1970, S. 64-73.

Buchholz, W. und Haslbeck, Ch. (1991): Private Verhandlungen und staatliche Regulierung bei asymmetrischer Information: Ein Wohlfahrtsvergleich, in: Finanzarchiv, N. F. 49/1991/92, S. 167-180.

Büchner, L. M. (1992): Die Produkt-(Produzenten)-Haftung im europäischen Vergleich unter Berücksichtigung der Haftung der Deutschen Bundespost Telekom, in: Archiv für Post und Telekommunikation 1992, H. 2, S. 103-112.

Büllesbach, A. (1995): Informationsverarbeitungssicherheit, Datenschutz und Qualitätsmanagement, in: Recht der Datenverarbeitung, 11/1995, H. 1, S. 1-6..

Bundesamt für Sicherheit in der Informationstechnik (1992): IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik, Version 1.0, Bonn 1992.

Bundesamt für Sicherheit in der Informationstechnik (1993): Zertifizierte IT-Produkte und Produktempfehlungen für die materielle Sicherheit, Bonn 1993.

Bundeskriminalamt (1994): Polizeiliche Kriminalstatistik Bundesrepublik Deutschland: Berichtsjahr 1993, Wiebaden 1994.

Bundesministerium für Post und Telekommunikation (1995): Eckpunkte eines künftigen Regulierungsrahmens im Telekommunikationsbereich, Bonn 1995.

Calabresi, G. (1970): The Costs of Accidents: A Legal and Economic Analysis, New Haven 1970.

Calabresi, G. und K. C. Bass (1970): Right Approach, Wrong Implications: A Critique of McKean on Products Liability, in: The University of Chicago Law Review, 38/1970, S. 74-91.

Cansier, D.(1993): Umweltökonomie, Stuttgart 1993.

Castelli, F. und Leporelli, C. (1993): Critical mass of users versus critical mass of services in a multiproduct information service system, in: Information Economics and Policy 5/1993, S. 331-355.

Chan, Y.-S. und Marino, A. M. (1994): Regulation of Product Safety Characteristics Under Imperfect Observability, in: Journal of Regulatory Economics 6/1994, S. 177-195.

Chang, Y.-M. und Ehrlich, I. (1985): Insurance, portection from risk, amd risk-bearing, in: Canadien Journal of Economics 18/1985, H. 3, S. 574-586.

Chiang, A. C. (1984): Fundamental Methods of Mathematical Economics, 3. Aufl., Singapur u. a. 1984.

Cicchetti, Ch. J. und Dubin, J. A. (1994): A Microeconometric Analysis of Risk Aversion and the Decision to Self-Insure, in: Journal of Political Economy, 102/1994, H. 1, S. 169-186.

Clark, D. E. und Cosgrove, J. C. (1990): Hedonic Prices, Identification, and the Demand for Public Safety, in: Journal of Regional Sceince, 30/1990, H. 1, S. 105-121.

Cleeton, D. L. und Zellner, B. B. (1993): Income, Risk Aversion, and the Demand for Insurance, in: Southern Economic Journal 60/1993, H. 1, S. 146-156.

Clotfelter, Ch. T. (1977): Public Services, Private Substitutes, and the Demand for Protection Against Crime, in: American Economic Review 67/1977, H. 5, S. 867-877.

Clotfelter, Ch. T. (1978): Private Security and the Public Safety, in: Journal of Urban Economics, 5/1978, S. 388-402.

Coase, R. (1960): The Problem of Social Cost, in: Journal of Law and Economics 3/1960, S. 1-44.

Cook, P. J. und D. A. Graham (1977): The Demand for Insurance and Protection: The Case of Irreplacable Commodities, in: The Quarterly Journal of Economics, 91/1977, S. 143-156.

Cooper, Th. E. (1992): Signal Facilitation: A Policy Response to Asymmetric Information, in: Journal of Business, 65/1992, H. 3, S. 431-450.

Cooter, R. D. (1991): Economic Theories of Legal Liability, in: Journal of Economic Perspectives 5/1991, H. 3, S. 11-30.

Cordewener, F. und Speckmann, R (Hrsg.) (1991): Auf dem Wege zur Informationsgesellschaft: Nutzen und Risiken neuer Kommunikationstechniken, Bremen 1991.

Cornes, R. und Sandler, T. (1986): The Theory of Externalities, Public Goods, and Club Goods, Cambridge N. Y. 1986.

Crandall, R. W.(1988): The Use of Cost-Benefit Analysis in Product Safety Regulation, in: The Frontier of Research in the Consumer Interest, hrsg. von E. Scott Maynes und dem ACCI Research Committee, Columbia 1988, S. 61-75.

Crandall, R. W. und Flamm, K (Hrsg.) (1989): Changing the Rules: Technological Change, International Competition, and Regulation in Communications, Washington, D. C., 1989.

Dardis, R. (1988): Risk Regulation and Consumer Welfare, in: Journal of Consumer Affairs 22/1988, H. 2, S. 303-318.

David, P. A. und Greenstein, S. (1990): The Economics of Compatibility Standards: An Introduction to Recent Research, in: Economics of Innovation and New Technologies 1/1990, S. 3-41.

David, P. A. und Steinmueller, W. E. (1994): Economics of compatibility standards and competition in telecommunication networks, in: Information Economics and Policy 6/1994, S. 217-241.

Deutscher Versicherungs-Schutzverband (1992): Wie Sie Ihre EDV-Risiken richtig versichern - Eine Anleitung für Betriebe - , 2. Auflage, Bonn 1992.

Diamond, P. A. und Mirrless, J. A. (1975): On the assignment of liablity: the uniform case, in: The Bell Journal of Economics 6/1975, S. 487-516.

Dionne, G. (1982): Moral Hazard and State-Dependent Utility Function, in: Journal of Risk and Insurance 49/1982, S. 405-422.

Dionne, G. und Eeckhoudt, L. (1985): Self-Insurance, Self-Protection and Increased Risk Aversion, in: Economics Letters 17/1985, S. 39-42.

Dixit, A. K. und Stiglitz, J. E. (1977): Monopolistic Competition and Optimum Product Diversity, in: American Economic Review 67/1977, S. 297-308.

Dorfman, R. (1970): The Economics of Products Liability: A Reaction to McKean, in: The University of Chicago Law Review, 38/1970, S. 92-102.

Douglas, M. und Wildavsky A. (1992): Risk and Culture - An Essay on the Selection of Technical and Environmental Dangers, Berkely u. a. 1992.

Ehlers, St. u. a. (1994): Telekommunikation: Dienste, Übersichten, Entscheidungshilfen, Berlin 1994.

Ehrlich, I. und G. S. Becker (1972): Market Insurance, Self-Insurance, and Self-Protection, in: Journal of Political Economy, 80/1972, S. 623-648.

Eichenberger, R. und Frey, B. S. (1990): Entscheidungsanomalien, in: Wirtschaftswissenschaftliches Studium, 19/1990, H. 6, S: 270-274

Einhorn, M. A. (1992): Mix and match compatibility with vertical product dimensions, in: The Rand Journal of Economics, 23/1992, S. 535-547.

Eisen, R. (1990): Problems of Equilibria in Insurance Markets with Asymmetric Information, in: Risk, Information and Insurance hrsg. von Loubergé, H., Boston u. a. 1990, S: 123-141.

Endres, A. (1991): Ökonomische Grundlagen des Haftungsrechtes, Heidelberg 1991.

Engels, P. (1991): So optimieren Sie ihre EDV-Versicherungen, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 1991, H. 6, S. 390-404.

Epple, D. und Raviv, A. (1978): Product Saftey: Liability Rules, Market Structure, and Imperfect Information, in: American Economic Review 68/1978, H. 1, S. 80-95.

Faure, M. und Van den Bergh R. (Hrsg.) (1989): Essays in Law and Economics: Corporations, Accident Prevention and Compensation for Losses, Antwerpen 1989.

Finsinger J. und Simon, J. (1989): An Economic Assesssment of the EC Prodcut Liability Directive and the Product Liability Law of the Federal Republic of Germany, in: Essays in Law and Economics: Corporations, Accident Prevention and Compensation for Losses hrsg. von Faure, M. und Van den Bergh, R., Antwerpen 1989, S. 185-214.

Fölling, W. F. (1994): Mobile Daten- und Telefaxübertragung in GSM-Netzen, in: Nachrichtentechnische Zeitung 47/1994, H. 8, S. 558-563.

Foray, D. (1994): Users, standards and the economics of coalitions and committees, in: Information Economics and Policy 6/1994, S. 269-293.

Forster, W. und Just, R. E. (1989): Measuring Welfare Effects of Product Contamination with Consumer Uncertainty, in: Journal of Environmental Economics and Management 17/1989, S. 266-283.

Franck, R. (1986): Rechnernetze und Datenkommunikation, Berlin, Heidelberg u. a. 1986.

Frey, B. S. und R. Eichenberger (1989): Zur Bedeutung entscheidungstheoretischer Anomalien für die Ökonomik, in: Jahrbücher für Nationalökonomie und Statistik, 206/1989, H. 2, S. 81-101.

Fritsch, M., Wein, Th. und Ewers, H.-J. (1993): Marktversagen und Wirtschaftspolitik: Mikroökonomische Grundlagen staatlichen Handelns, München 1993.

Frost & Sullivan (1992): The European Market for Information Technology (IT) Security Products & Services, New York 1992. (Unveröffentlichte Studie).

Fuhrberg, K. (1995): Sicherheit auf der Datenautobahn, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Einführung, S. 1-11.

Fumy, W. und Riess, H. P. (1993): Netzsicherheit durch Verschlüsselungsmethoden, in: Computer und Recht 9/1993, H. 2, S. 117-124.

Gal-Or, E.(1983): Quality and quantity competition, in: The Bell Journal of Economics, 14/1983, S. 590-600.

Garbe, D. (1991): Privacy und Gesellschaft: Eine spannungsvolle Beziehung in: Technikfolgenabschätzung in der Telekommunikation hrsg. von Garbe, D. und Lange, K., Berlin, Heidelberg u. a. 1991, S. 107-120.

Garbe, D. (1992): Datenspuren in digitalisierten Telekommunikationsnetzen: Ein Vergleich der Datenschutzregelungen in europäischen Ländern am Fall ISDN, Diskussionsbeitrag Nr. 103 des WIK, Bad Honnef 1992.

Garstka, H. (1993): Probleme aus der Sicht des Datenschutzes, in: Daten- und Verbraucherschutz bei Telekommunikationsdienstleistungen in der EG hrsg. von Kubicek, H., Baden-Baden 1993, S. 32-36.

Gartner H. A. und Konrad, P. (1994): KES-Sicherheits-Studie 1994: So sehen DV-Betreiber ihre Sicherheit, in: Sonderdruck der Zeitschrift für Kommunikations- und EDV-Sicherheit 1994, H. 3, S. 2-15.

Gauthey, F. und Haefelfinger, R. (1991): Sicherheit in der Datenkommunikation, in: io Management Zeitschrift 60/1991, H. 6, S. 67-70.

Geißler, B. (1993): Produkthaftung - Eine ökonomische Analyse unter Berücksichtigung wohlfahrtstheoretischer, wettbewerblicher und evolutorischer Aspekte, Würzburg 1993.

Gerke, P. R. (1991): Digitale Kommunikationsnetze: Prinzipien, Einrichtungen, Systeme, Berlin, Heidelberg u. a. 1991.

Gerner, J. L.(1988): Product Safety: A Review, in: The Frontier of Research in the Consumer Interest hrsg. von E. Scott Maynes und dem ACCI Research Committee, Columbia 1988, S. 37-59.

Gilmore, G.: Products Liability: A Commentary, in: The University of Chicago Law Review, 38/1970, S. 103-116.

Gray, W. B. (1987): The Cost of Regulation: OSHA, EPA and the Productivity Slowdown, in: American Economic Review 77/1987, H. 5, S. 998-1006.

Greenwald, B. C. und Stiglitz, J. E. (1986): Externalities in Economies with Imperfect Information and Incomplete Marktes, in: The Quarterly Journal of Economics 101/1986, S. 229-264.

Groebel, J. (1994): Der Markt wird's nicht richten, in: Die Zeit, Nr. 42, 14. 10. 1994, S. 78.

Gronert, E. (1995): Der Trend geht zum Zweittelefon, in: Das Handelsblatt, 19. 4. 1995, S. 29.

Gruenspecht, H. K. und Lavé, L. B. (1989): The Economics of Health, Safety, and Environmental Regulation, in: Handbook of Industrial Organization, Volume II, hrsg. von Schmalensee R. und Willig R. D., Amsterdam u. a. 1989, S. 1507-1550.

Hamada, K. (1976): Liability Rules and Income Distribution in Product Liablity, in: American Economic Review 66/1976, H. 1, S. 228-234.

Hammer, V. (1991): Verletzlichkeit und Verfassungsverträglichkeit technischer Verfahren zur Datensicherung, in: Technikfolgenabschätzung in der Telekommunikation hrsg. von Garbe D. und Lange K., Berlin 1991, S. 131-139.

Hauser, H. (1979): Qualitätsinformationen und Marktstrukturen, in: Kyklos 32/1979, H. 4, S. 739-763.

Hayashi, K. (1993): Information infrastructure: Who builds broadband networks?, in: Information Economics and Policy 5/1993, S. 295-309.

Head, J. G. (1966): On Merit Goods, in: Finanzarchiv N. F. 25/1966, S. 1-29.

Head, J. G. (1969): Merit Goods Revisited, in: Finanzarchiv N. F. 28/1969, S. 214-225.

Heal, G. (1989): Price and Market Share Dynamics in Network Industries, First Boston Working Paper Series, Boston 1989, S. 1-26.

Heidinger, J. L. (1980): Die Computer-Mißbrauch-Versicherung, Karlsruhe 1980.

Heidinger, J. L. und Andrich R. (1987): Datensicherung im Unternehmen: Sicherheitsprogramm gegen Datenmißbrauch und Wirtschaftskriminalität, Landsberg 1987.

Heinlin, I. (1993): Individuelle Zahlungsbereitschaft für Versicherungsschutz und Messung der Risikoeinstellung bei der Versicherungsentscheidung: Eine entscheidungstheoretische Analyse, Frankfurt/Main u. a. 1993.

Heuser, A. (1995): Verschlüsselungssysteme: Bedrohungen und Anforderungen, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Einführung, S. 1-5.

Hiebert, L. D. (1983): Self Insurance, Self Protection and the Theory of the Competitive Firm, in: Southern Economic Journal 50/1983, S. 160-168.

Hirshleifer, J. und Riley, J. G. (1992): The Analytics of Uncertainty and Information, Cambridge 1992.

Hirshleifer, J. und Glazer, A. (1992): Price Theory and Applications, Englewood Cliffs 5. Aufl. 1992.

Höller, H. (1993): Europäische Normungspolitik: Bedeutung für die Kommunikationstechnik, in: Computer und Recht 9/1993, H. 1, S. 40-46.

Horster, P. und Portz, M. (1994): Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, in: Datenschutz und Datensicherung 1994, H. 8, S. 434-442.

Jones-Lee, M. W.(1989): The Economics of Safety and Physical Risk, Oxford u. a. 1989.

Jones-Lee, M. W. (1990): The Value of Transport Safety, in: Oxford Review of Economic Policy 6/1990 , H. 2, S. 39-60.

Jovanovic, B.(1982): Truthful disclosure of information, in: The Bell Journal of Economics, 13/1982, S. 36-44.

Kahneman, D., Slovic, P. und A. Tversky (Hrsg.) (1991): Judgement under uncertainty: Heuristics and biases, Cambridge, New York, u. a. 1991.

Kahneman, D. und A. Tversky (1991): On the psychology of prediction, in: Judgement under uncertainty: Heuristics and biases hrsg. von Kahneman, D. u.a., Cambridge 1991, S. 48-68.

Kahneman, D. und Tversky, A. (1991): Availability: A heuristic for judging frequncy and probability, in: Judgement under uncertainty: Heuristics and biases hrsg. von Kahneman D. u. a., Cambridge 1991, S. 163-178.

Kampmann, F. (1993): Wettbewerbsanalyse der Normung der Telekommunikation in Europa, Frankfurt am Main 1993.

Kates, R. W. (1976): Risk Assessment of Environmental Hazard, Scope Report No. 8, International Council of Scientific Unions, Paris 1976.

Katz, J. (1991): Privacy in der Telekommunikation: Trends und Probleme, in: Technikfolgenabschätzung in der Telekommunikation hrsg. von Garbe D. und Lange K., Berlin 1991, S. 55-69.

Katz, M. L. und Shapiro, C. (1985): Network Externalities, Competition, and Compatibility, in: American Economic Review 75/1985, H. 3, S. 424-440.

Kim, J. Ch. (1985): The Market for „Lemons" Reconsidered: A Model of the Used car Market with Asymmetric Information, in: American Economic Review 75/1985, H. 4, S. 836-843.

Kindleberger, Ch. P. (1983): Standards as Public, Collective and Private Goods, in: Kyklos 36/1983, H. 3, S. 377-396.

Klaver, F. und Slaa, P. (1992): Telecommunication: New Signposts to Old Roads, Amsterdam, Oxford u. a. 1992.

Klein, B. und Leffler, K. B. (1981): The Role of Market Forces in Assuring Contractual Performance, in: Journal of Political Economy 89/1981, H. 4, S. 615-641.

Knieps, G. (1994): Standardization: The Evolution of Institutions versus Government Intervention, Discussion Paper 10, Freiburg 1994.

Knight, F. H. (1921): Risk, Uncertainty and Profit, New York 1921.

Knorr, H. (1993): Öknomische Probleme von Kompatibilitätsstandards: Eine Effizienzanalyse unter besonderer Berücksichtigung des Telekommunikationsbereichs, Baden-Baden 1993.

Koboldt, Ch., Leder, M. und Schmidtchen, D. (1992): Ökonomische Analyse des Rechts, in: Wirtschaftswissenschaftliches Studium 21/1992, H. 7, S. 334-342.

Kolmogoroff, A. N. (1933): Grundbegriffe der Wahrscheinlichkeitsrechnung, Berlin 1933.

Kolstad, Ch. D., Ulen Th. S. und Johnson G. V.(1990): Ex Post Liability for Harm vs. Ex ante Safety Regulation: Substitutes or Complements?, in: American Economic Review, 80/1990, H. 4 S. 888-901.

Kommission der Europäischen Gemeinschaften (1992): Sicherer EDI-Verkehr - Ein Management-Brevier, Luxemburg 1992.

Kowalski, B. und Wolfenstetter, K.-D. (1994): Sicherheitsstandards im Rahmen der ETSI-Normungsarbeiten, in: Datenschutz und Datensicherung 1994, H. 1, S. 30-38.

Kubicek, H. (1991): ISDN, Privacy und Datenschutz - Anmerkungen zur aktuellen Diskussion in den USA und in der BRD, in: Technikfolgenabschätzung in der Telekommunikation, hrsg. von Garbe, D. und Lange K., Berlin, Heidelberg u. a. 1991, S. 70-105.

Kubicek, H. (1991a): Neue Risiken - Neue Regulierungsaufgaben, in: Auf dem Wege zur Informationsgesellschaft: Nutzen und Risiken neuer Kommunikationstechniken hrsg. von Cordewener, F. und Speckmann, R., Bremen 1991, S. 44-58.

Kubicek, H. (Hrsg.) (1993): Daten- und Verbraucherschutz bei Telekommunikationsdienstleistungen in der EG, Baden-Baden 1993.

Kubicek, H. und Berger P. (1990): Was bringt uns die Telekommunikation? ISDN - 66 kritische Fragen, Frankfurt 1990.

Kündig, A. (1989): Datensicherheit in vernetzten Systemen, in: io Management Zeitschrift 58/1989, H. 10, S. 74-78.

Kuhlmann, E.(1990): Verbraucherpolitik: Grundzüge ihrer Theorie und Praxis, München 1990.

Kunz, H. (1993): Kriminalität, in: Ökonomische Verhaltenstheorie hrsg. von Ramb, B.-Th. und Tietzel, M. München 1993, S. 181-206.

Lancaster, K. (1975): Socially Optimal Product Differentiation, in: American Economic Review 65/1975, H. 4, S. 567-585.

Lavé, L. B.: Safety in Transportation: The Role of Government, in: Law and Contemporary Problems, 33/1968, S. 512-535.

Leiberich, O. (1995): Verschlüsselung und Kriminalität - eine Bedrohung, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Einführung, S. 1-7.

Leland, H. E. (1979): Quacks, Lemons, and Licensing: A Theory of Minimum Quality Standards, in: Journal of Politcal Economy 87/1979, H. 6, S. 1328-1346.

Levy, St. (1994): Bericht vom Kryptokrieg, in: Die Zeit, Nr. 1, 30. 12. 1994, S. 54.

Lewis, T. und Nickerson, D. (1989): Self-Insurance against Natural Disasters, in: Journal of Environmental Economics and Management 16/1989, S. 209-223.

Liebowitz, S. J. (1983): Tie-In Sales and Price Discrimination, in: Economic Inquiry 21/1983, S. 387-399.

Liebowitz, S. J. und Margolis, St. E. (1994): Network Externality: An Uncommon Tragedy, in: Journal of Economic Perspectives, 8/1994, H. 2, S. 133-150.

Littlechild, St. C. (1975): Two-part tariffs and consumption externalities, in: The Bell Journal of Economics 4/1975 H. 2, S. 661-670.

Lucius, R.-R. (1979): Die Grenzen der Versicherbarkeit, Frankfurt 1979.

Lütge, G. (1995): Eldorado für Piraten, in: Die Zeit Nr. 6, 3. 2. 1995, S. 19f.

Lunn, J. (1990): Tie-in Sales and the Diffusion of New Technology, in: Journal of Institutional and Theoretical Economics 146/1990, S. 249-260.

Machina, M. J. (1987): Choice Under Uncertainty: Problems Solved and Unsolved, in: Journal of Economic Perspectives 1/1987, H. 1, S. 121-154.

MacLean, D. J. (1995): A new departure for the ITU: An inside view of the Kyoto Plenipotentiary Conference, in: Telecommunications Policy 19/1995, H. 3, S. 177-190.

Macpherson, A. (1990): International Telecommunication Standards Organizations, Boston 1990.

Manne, H. G.(1970): Edited Transcript of AALS-AEA Conference on Products Liability, in: The University of Chicago Law Review, Vol. 38, 1970, S. 117-141.

Maynes, E. Scott (Hrsg.) (1988): The frontier of research in the consumer interest, Columbia 1988.

Magat, W. A. und W. Kip Viscusi (1992): Informational Approaches to Regulation, Cambridge, Ma., 1992.

Magoulas, G. (1985): Zur ökonomischen Analyse des Konsumentenschutzes - unter Berücksichtigung informations- und risikobezogerenr Probleme von Konsumentenmärkten, in: Recht und Ökonomie beim Konsumentenschutz und Konsumentenrecht hrsg. von Simon, J., Baden-Baden 1985, 23-57.

Magoulas, G. (1988): Staatseingriffe bei externen Effekten und asymmetrischer Informationsverteilung - Am Beispiel des Umwelt und Konsumentschutzes, in: Recht und Risiko hrsg. von Finsinger J. und Simon, J., München 1988, S. 66-93.

Matthews St. und A. Postlewaite (1985): Quality testing and disclosure, in: The Rand Journal of Economics, 16/1985, S. 328-340.

Matutes, C. und Regibeau, P. (1992): Compatibility and Bundling of Complemetary Goods in a Duopoly, in: The Journal of Industrial Economics 40/1992, S. 37-54.

McKean, R. N. (1970): Products Liability: Implications of Some Changing Property Rights, in: The Quarterly Journal of Economics, 84/1970, S. 611-626.

McKean, R. N. (1970a): Products Liability: Trends and Implications, in: The University of Chicago Law Review, 38/1970, H. 3, S. 3-63.

Meyer, D. (1990): Asymmetrische Information, Institutional Choice und die Funktion von Wertorientierungen, in: Jahrbuch für Sozialwissenschaft, 41/1990, S. 104-121.

Meyer-Reim, U. (1992): Die Elektronik-Versicherung: Sachversicherung von Fernmelde- und sonstigen elektrotechnischen Anlagen, Frankfurt/Main 1992.

Milde, H. (1988): Die Theorie der adversen Selektion, in: Wirtschaftswissenschaftliches Studium, 17/1988, H. 1, S. 1-6.

Millin, N. (1994): Weltweite Kommunikation über Internet, in: Nachrichtentechnische Zeitung 47/1994, H. 10, S. 704-712.

Mitchell, B. und Vogelsang, I, (1994): Interconncetion of Telecommuications Networks in the USA, Diskussionsbeitrag Nr. 138 des WIK, Bad Honnef 1995.

Molitor, B. (1987): Meritorisierung des Gutes „Sicherheit"?, in: Grundtexte zur Sozialen Marktwirtschaft, Band 2, hrsg. von Hohmann K. u. a., Stuttgart 1988, S. 417-425.

Moser, A. (1995): Aspekte der Kosten-Effektivität von Datensicherungskonzepten, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Sektion 1, S. 1-11

Moses, L. N. und Savage I. (Hrsg.) (1989): Transportation Safety in an Age of Deregulation, New York und Oxford 1989.

Müller, G. (1994): Schöne neue Telewelten? Das thematische Umfeld des neuen Kollegs „Sicherheit in der Kommunikationstechnik", in: Info-Sonderdruck 4/1994, S. 1-3.

Müller, G. (1994a): Security as Integral Part of Telecomm Services, Arbeitspapier, Universität Freiburg, Institut für Informatik und Gesellschaft, Abteilung Telematik, Freiburg 1994.

Mulgan, G. J. (1991): Communication and Control: Networks and the New Economics of Communication, Oxford 1991.

Näther, B. (1991): Verlässliche Informationstechnik, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 2/1991, S. 78-86.

National Research Council (1989): Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness, Board on Telecommunications and Computer Applications, Washington D. C. 1989.

Nell, M. (1993): Versicherungsinduzierte Verhaltensänderungen von Versicherungsnehmern, Karlsruhe 1993.

Nelson, P. (1970): Information and Consumer Behavior, in: Journal of Political Economy, 78/1970, S. 311-329.

Neumann, J. v. und Morgenstern, O. (1944): Theory of Games and Economic Behavior, Princeton N. J. 1944.

Netzer, B. (1995): Daten her, sonst knallt's!, in: Die Zeit 1995, Nr. 8, 17. 2. 1995, S. 82.

Noam, E. M. (1991): Privacy bei Telekommunikationsdiensten, in: Telekommunikation und Gesellschaft, Kritisches Jahrbuch der Telekommunikation, hrsg. von Kubicek H., Karlsruhe 1991, S. 112-131.

Noam, E. M.(1992): Telecommunications in Europe, Oxford, N. Y., 1992.

Noam, E. M.(1992a): A Theory for the Instability of Public Telecommunications systems, in: The Economics of Information Networks hrsg. von Antonelli, C., Amsterdam 1992, S. 107-127.

o. V. (1992): Neues aus dem BSI, in: Zeitschrift für Kommunikations- und EDV-Sicherheit, 1992, H. 2, S. 133.

o. V. (1993): Sicherheit gewinnt an Bedeutung, in: Zeitschrift für Kommunikations- und EDV-Sicherheit, 1993, H. 3, S. 8.

o. V. (1994): Mobilfunkfirmen durch Betrug geschädigt, in: Das Handelsblatt, 4. 8. 1994, S. 1.

o. V. (1994a): Integrierte Schutzkonzepte liegen voll im Trend, in: Das Handelsblatt, 5. 10. 1994, S. 29.

o. V. (1994b): Investitionen für die Telekommunikation, in: Die Zeit Nr. 41, 7. 10. 1994, S. 26.

o. V. (1995): Durch TV-Kabelnetze 140000 neue Arbeitsplätze, in: Das Handelsblatt, 2. 1. 1995, S. 13

o. V. (1995a): Vorläufiges Ergebnis des US-Marktes, in: Das Handelsblatt, 4. 1. (1995), S. 11.

o. V. (1995b): Die Industrie lagert Werkschutz aus, in: Das Handelsblatt, 12. 1. 1995, S. 12.

o. V. (1995c): Die „zweite industrielle“ Revolution muß politisch flankiert werden, in: Die Badische Zeitung, 25. 2. 1995, S. 3.

o. V. (1995d): D-Netz soll abgehört werden können, in: Das Handelsblatt, 23. 3. 1995, S. 3.

o. V. (1995e): Viele Ausweichmöglichkeiten für Kriminelle, in: Das Handelsblatt, 2. 5. 1995, S. 13.

Oakland, W. H. (1987): Theory of Public Goods, in: Handbook of Public Economics Volume II hrsg. Auerbach, A. J. und Feldstein, M., Amsterdam u. a. 1987, S. 485-535.

Oi, W. (1973): The Economics of Product Safety, in: The Bell Journal of Economics and Management, 4/1973, S. 3-29.

Oi, W. (1974): On the Economics of Industrial Safety, in: Law and Contemporary Problems, 38/1974, S. 669-699.

Oren, S. S. und Smith, St. A. (1981): Critical mass and tariff structure in electronic communications marktes, in: The Bell Journal of Economics, 12/1981, H. , S. 467-487.

Ott, C. und Schäfer, H.-B. (Hrsg.) (1989): Allokationseffizienz in der Rechtsordnung, Berlin, Heidelberg u. a. 1989.

Overgaard, P. B. (1992): Adverse Producer Incentives and Product Quality When Consumers Are Short-term Players, in: Journal of Economics, 55/1992, H. 2, S. 169-191.

Paszkowsky, I. (1995): Kein anderes Verfahren ist so flexibel und leistungsfähig, in: Das Handelsblatt Nr. 76 vom 19. 4. 1995, S. 27.

Pauly, M. V. (1974): Overinsurance and Public Provision of Insurance: The Roles of Moral hazard and Adverse Selection, in: Quarterly Journal of Economics, 88/1974, S. 44-62.

Peltzman S. (1976): The Effects of Automobile Safety Regulation, in: Journal of Political Economy 83/1975 H. 4, S. 677-725.

Perels, J. (Hrsg.) (1979): Grundrechte als Fundament der Demokratie, Frankfurt/Main 1979.

Peters, H. (1995): Informationstechnische Sicherheitsbedürfnisse und Sicherheitsmechanismen in der Mobilkommunikation, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Sektion 4, S. 1-11.

Petersen, D. (1994): Privatfirmen bewachen jetzt auch Gefängnisse, in: Das Handelsblatt, 12. 10. 1994, S. 17.

Petersen, D. (1994a): Gewaltmonopol, in: Das Handelsblatt, 17. 10. 1994, S. 10.

Pfitzmann, A. (1990): Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz, Berlin, Heidelberg u. a. 1990.

Pfitzmann, A. (1993): Technischer Datenschutz in öffentlichen Funknetzen, in: Datenschutz und Datensicherung 1993, H. 8, S. 451-463.

Pfitzmann, A. und Rannenberg K. (1993): Staatliche Initiativen und Dokumente zur IT-Sicherheit: Eine kritische Würdigung, in: Computer und Recht 9/1993, H. 3, S. 170-179.

Podlech, A. (1979): Das Recht auf Privatheit, in: Grundrechte als Fundament der Demokratie hrsg. von Perels J., Frankfurt/Main 1979, S. 50-68.

Pohl, H. und Weck, G. (1993): Stand und Zukunft der Informationssicherheit, in: Datenschutz und Datensicherung 1993, H. 1, S. 18-22 und H. 2, S. 78-86.

Pohl H. und Weck, G. (1993a): Einleitung: Stand und Zukunft der Informationssicherheit, in: Einführung in die Informationssicherheit hrsg. von Pohl, H. und Weck, G., München 1993, S. 9-31.

Polinsky, A. M. und W. P. Rogerson (1983): Products liability, consumer misperceptions, and market power, in: The Bell Journal of Economics, 14/1983, S. 581-589.

Pommerehne, W. W. (1987): Präferenzen für öffentliche Güter: Ansätze zu ihrer Erfassung, Tübingen 1987.

Posner, R. A. (1974): Theories of Economic Regulation, in: The Bell Journal of Economics and Management Science 5/1974, S. 335-358.

Posner, R. A.(1981): The Economics of Privacy, in: American Economic Review 71/1981, H. 2, S. 404-409.

Pratt, J. W. (1964): Risk Aversion in the Small and in the Large, in: Econometrica 32/1964, S. 122-136.

Priddat, B.P. (1992): Zur Ökonomie der Gemeinschaftsbedürfnisse: Neuere Versuche einer ethischen Begründung der Theorie meritorischer Güter, in: Zeitschrift für Wirtschafts- und Sozialwissenschaften, 112 (1992), S. 239-259.

Priest, G. L. (1991): The Modern Expansion of Tort Liablity: Its Sources, Its Effects, and Its Reform, in: Journal of Economic Perspectives 5/1991, H. 3, S. 31-50.

Quiggin, J. (1992): Risk, Self-Protection and Ex Ante Economic Value - Some Positive Results, in: Journal of Environmental Economics and Management 23/1992, S. 40-53.

Rannenberg, K. (1994): Recent Development in Information Technology Security Evaluation - The Need for Evaluation Criteria for multilateral Security, in: Security and Control of Information Technoligy in Society hrsg. von Sizer, R. u. a. Amsterdam 1994, S. 113-128.

Rapold, I. (1988): Qualitätsunsicherheit als Ursache von Marktversagen - Anpassungsmechanismen und Regulierungsbedarf, München 1988.

Recktenwald, H. C. (1967): Effizienz und Innere Sicherheit, in: Kyklos 20/1967, S. 607-641.

Rejda, G. E. (1992): Principles of Risk Management and Insurance, 4. Aufl. New York 1992.

Richter, A. (1995): Adverse Selektion auf Versicherungsmärkten: Informationsökonomische Analyse bei exogener, vom Versicherer nicht beobachtbarer Schadenverteilung, Karlsruhe 1995.

Rihaczek, K. (1993): Kryptoalgorithmen in offenen Koomunikationssystemen: Notwendigkeit und Gefahren ihrer Normung, in: Datenschutz und Datensicherung 1993, H. 4, S. 220-226.

Rihaczek, K. (1994): Vertraulichkeit im Telekommunikationssystem, in: Datenschutz und Datensicherung 1994, H. 8, S. 512.

Risa, A. E. (1992): Public Regulation of Private Accident Risk: The Moral Hazard of Technological Improvement, in: Journal of Regulatory Economics, 4/1992, S. 335-346.

Rohlfs, J. (1975): A theory of interdependent demand for a communications service, in: The Bell Journal of Economics 5/1975, H. 1, S. 16-37.

Rose, N. L. (1990): Profitability and Product Quality: Economic Determinants of Airline Safety Performance, in: Journal of Political Economy, 98/1990, H. 5, S. 944-964.

Rose, N. L. (1992): Fear of Flying? Economic Analysis of Airline Safety, in: Journal of Economic Perspectives 67/1992, H. 2, S. 75-94.

Rosenbaum, U. und Sauerbrey, J. (1995): Bedrohungs- und Risikoanalysen bei der Entwicklung sicherer IT-Systeme, in: Datenschutz und Datensicherung 1995, H. 1, S. 28-34.

Roßnagel, A.(1984): Rechtliche Risikosteuerung. Kritik und Alternativen, in: Recht und Technik im Spannungsfeld der Kernenergiekontroverse hrsg. v. Roßnagel A., Opladen 1984, S. 198-220.

Roßnagel, A., Wedde, P., Hammer, V. und Pordesch, U. (1989): Die Verletzlichkeit der Informationsgesellschaft, Opladen 1989.

Roy, R. (1995): Datenschutzrechtliche Aspekte bei der Privatiiserung der Deutschen Bundespost, in: Datenschutz und Datensicherung 1995, H. 3, S. 135-136.

Rueppel, R. A. (1994): „Clipper“ - Der Krypto-Konflikt am Beispiel der Amerikanischen ESCROW Technologie, in: Datenschutz und Datensicherung 1994, H. 8, S. 443- 451.

Samuleson, P. A. (1954): The Pure Theory of Public Expenditure, in: The Review of Economics and Statistics 36/1954, S. 387-389.

Samuleson, P. A. (1955): Diagrammatic Exposition of a Theory of Public Expenditure, in: The Review of Economics and Statistics 37/1955, S. 350-356.

Savage, L. J. (1954): The Foundations of Statistics, New York 1954.

Schadow, H. (1991): Neues Datenschutzrecht ud Poststrukturgesetz, in: Archiv für Post und Fernmeldewesen 43/1991, H. 4, S. 444-467.

Schäfer, H.-B. (1993): Ökonomische Analyse des Rechts, in: Ökonomische Verhaltenstheorie hrsg. von Ramb, B.-Th. und Tietzel, M. München 1993, S. 149-180.

Schäfer, H.-B. und Ott, C. (1986): Lehrbuch der ökonomischen Analyse des Zivilrechts, Berlin, Heidelberg u. a. 1986.

Schau, v., P. (1994): Entwicklung der Telekommunikationsnetze: Markt und Technik im Wandel, in: Nachrichtentechnische Zeitung 47/1994, H. 3, S. 146-152.

Schlesinger, H. (1984): Optimal Insurance for Irreplacable Commodities, in: Journal of Risk and Insurance, 51/1984, S. 131- 137.

Schlette, J. (1992): Risikoanalyse für PC-/LAN-Umgebungen, in: Datenschutz und Datensicherung 1992, H. 3, S. 136-144.

Schneider, J. (1993): Die EG-Richtlinie zum Datenschutz, in: Computer und Recht 9/1993, H. 1, S. 35-39.

Schoder, D. (1995): Diffusion von Telekommunikationsdiensten: Phänomenologie und Erklärung, noch unveröffentliche Dissertation der Wirtschaftswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg im Breisgau 1995.

Schöppe, G. (1983): Consumer Protection by Law and Information: A View of Western German Practice and Experience, in: Journal of Institutional and Theoretical Economics, 139/1983, S. 545-567.

Schopka, K. (1994): Elektronik-Versicherungen: Wirtschaftlichkeit und Sparmöglichkeiten, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 1994, H. 6, S. 7-12.

Schützig, R. (1992): Vernetzte Systeme - eine Herausforderung für die Datensicherheit, in Nachrichtentechnische Zeitung 45/1992, H. 8, S. 616-621.

Schulenburg, v. d. Graf J. M. (1992): Versicherungsökonomik, in: Wirtschaftswissenschaftliches Studium 21/1992, H. 8, S. 399-406.

Schulenburg, v. d. Graf J. M. (1993): Marktprozeß und Marktstruktur bei unvollständiger Information, in: Zeitschrift für Sozial- und Wirtschaftswissenschaften 113(1993), S. 509-555.

Schulze Schwienhorst, M. (1995): Die Software-Haftpflichtversicherung, in: Computer und Recht 11/1995, H. 4, S. 193-198.

Schwab, R. M. und Zampelli, E. M. (1987): Disentangling the Demand Function from the Production Function for Local Public Services: The Case of Public Safety, in: Journal of Public Economics 33/1987, S. 245-260.

Shapiro, C. (1982). Consumer information, product quality, and seller reputation, in: The Bell Journal of Economics, 13/1982, S. 20-35.

Shapiro, C. (1983): Consumer Protection Policy in the United States, in: Journal of Institutional and Theoretical Economics, 139/1983, S. 527-544.

Shapiro, C. (1983a): Premiums for High Quality Products as Returns to Reputations, in: The Quarterly Journal of Economics, 98/1983, S. 659-679.

Shapiro, C. (1991): Symposium on the Economics of Liability, in: Journal of Economic Perspectives, 5/1991, H. 3, S. 3-10.

Shavell, St. (1979): On Moral Hazard and Insurance, in: Quarterly Journal of Economics 93/1979, S. 541-562.

Shavell, St.(1982): On liability and insurance, in: The Bell Journal of Economics, 13/1982, S. 120-132.

Shavell, St.(1984): Liability for Harm Versus Regulation of Safety, in: Journal of Legal Studies, 13/1984, S. 357-374.

Shavell, St. (1984a): A Model of the Optimal Use of Liability and Safety Regulation, in: The Rand Journal of Economics, 15/1984, H. 2 S. 271-280.

Shavell, St.(1987): Economic Analysis of Accident Law, Cambridge, MA, 1987.

Shioshansi, F. P. (1982): Insurance for Irreplacable Commodities, in: Journal of Risk and Insurance, 49/1982, S. 309-320.

Shogren, J. F. und Crocker, Th. D. (1991): Risk, Self-protection, and Ex Ante Economic Value, in: Journal of Environmental Economics and Management 20/1991, S. 1-15.

Sieber, U. (1995): Computerkriminalität und Informationsstrafrecht: Entwicklungen in der internationalen Informations- und Risikogesellschaft, in: Computer und Recht 11/1995, H. 2, S. 100-113.

Simon, M. J. (1981): Imperfect information, costly litigation, and product quality, in: The Bell Journal of Economics, 12/1981, S. 171-184.

Sinn, H.-W. (1980): Ökonomische Entscheidungen bei Ungewißheit, Tübingen 1980.

Skogh, G. (1989): The Combination of Private and Public Regulation of Safety, in: Essays in Law and Economics: Corporations, Accident Prevention and Compensation for Losses, hrsg. von M. Faure und. Van den Bergh, R, Antwerpen 1989, S. 87-101.

Spence, M. (1975): Monopoly, quality, and regulation, in: The Bell Journal of Economics, 6/1975, S. 417-429.

Spence, M. (1977): Consumer Misperceptions, Product Failure and Producer Liability, in: Review of Economic Studies 44/1977, S.561-572.

Spengler, J. J. (1968): The Economics of Safety, in: Law and Contemporary Problems, 33/1968, S. 619-638.

Spremann, K. (1990): Asymmetrische Information, in: Zeitschrift für Betriebswirtschaft 60/1990, H. 5/6, S. 561-586.

Squire, L. (1973): Some aspects of optimal pricing for telecommunications, in: The Bell Journal of Economics, 4/1973, H. 2, S. 515-525.

Starr, Ch. (1969): Social Benefit Versus Technological Risk: What is our Society Willing to Pay for Safety?, in: Science, 165/1969, S. 1232-1238.

Statistisches Bundesamt (1994), Statistisches Jahrbuch 1994 für die Bundesrepublik Deutschland, Wiesbaden 1994.

Staudinger, B. (1995): Sicherer Datentransfer in heterogenen Netzen, in: Fachvorträge: 4. Deutscher IT-Sicherheitskongreß 8. bis 11. Mai 1995, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 1995, Sektion 4, S. 1-7.

Stelzer, D. (1993): Sicherheitsstrategien in der Informationsverarbeitung: ein wissenbasiertes, objektorientiertes System für die Risikoanalyse, Wiesbaden 1993.

Stigler, G. J. (1971): The Theory of Economic Regulation, in: The Bell Journal of Economics and Management Sceince, 2/1971, S. 3-21.

Stiglitz, J. E. (1979): Equilibrium in Product Marktes with Imperfect Information, in: American Economic Review 69/1979, H. 2, S. 339-345.

Stoetzer, M.-W. (1991): Der Markt für Mehrwertdienste: Ein kritischer Überblick, Diskussionsbeitrag Nr. 69 des WIK, Bad Honnef 1991.

Stoetzer, M.-W. (1994): New telecommunication services: Current situation and prospects in Germany, in: Telecommunications Policy 18/1994, H. 7, S. 522-537.

Strassl, W. (1988): Externe Effekte auf Versicherungsmärkten: Eine allokationstheoretische Begründung staatlicher Regulierung, Tübingen 1988.

Streissler, E. (1993): Das Problem der Internalisierung, in: Umweltverträgliches Wirtschaften als Problem von Wissenschaft und Politik, hrsg. von H. König, Berlin 1993, S. 87-110.

Stuart, Ch. (1981): Consumer protection in markets with informationally weak buyers, in: The Bell Journal of Economics, 12/1981, S. 562-573.

Sweeney, G. H. und Beard, T. R. (1992): The Comparative Statics of Self-Protection, in: Journal of Risk and Insurance 59/1992, H. 2, S. 301-309.

System Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council (1991): Computers at Risk: Safe Computing in the Information Age, 3. Auflage, Wahington D. C. 1991.

TELA Versicherung (1994): Software versichern, München 1994.

Tiebout, Ch. (1956): A Pure Theory of Local Expenditures, in: Journal of Political Economy, 64/1956, H. 5, S. 414-424.

Tirole, J.(1988): The Theory of Industrial Organization, Cambridge, MA, 1988.

Traynor, Th. L. und McCarthy P. S. (1991): Trucking Deregulation and Highway Safety: The Effect of the 1980 Motor Carrier Act, in: Journal of Regulatory Economics, 3/1991, S. 339-348.

Tyler, M., Letwin, W. und Roe, Ch. (1995): Universal service and innovation in telecommunication services, in: Telecommunications Policy 19/1995, S. 3-20.

Ulrich, O. (1995): Dynamisch bis zum Absturz, in: Die Zeit Nr. 15, 7. 4. 1995, S. 33.

Ungerer, H. (1993): Einführung in die EG-Telekommunikationspolitik, in: Daten- und Verbraucherschutz bei Telekommunikationsdienstleistungen in der EG hrsg. von Kubicek, H. Baden-Baden 1993, S. 23-31.

Vahrenkamp, K. (1991): Verbraucherschutz bei asymmetrischer Information - Informationsökonomische Analysen verbraucherpolitischer Maßnahmen, München 1991.

VanDeVeer, D. (1986): Paternalistic Intervention, Princeton 1986.

Varian, H. R.(1992): Microeconomic Analysis, 3. Auflage, New York und London 1992.

Verhorn, Ch. L. (1979): Market Interaction between Public and Private Goods: The Demand for Fire Protection, in: The National Tax Journal 32/1979, S. 29-39.

Viscusi, W. Kip (1978): A note on "lemons" markets with quality certification, in: The Bell Journal of Economics, Vol. 9, 1978, S. 275-279.

Viscusi, W. Kip (1984): The Lulling Effect: The Impact of Child-Restistant Packaging on Aspirin and Analgesic Ingestions, in: American Economic Review, Papers and Proceedings 74/1984, H. 2, S. 324-327.

Viscusi, W. Kip (1984a): Regulating consumer product safety, Washington D. C. 1984.

Viscusi, W. Kip (1985): Consumer Behaviour and the Safety Effects of Product Safety Regulation, in: Journal of Law and Economics, 28/1985, S. 527-553.

Viscusi, W. Kip (1985a): Market Incentives for Safety, in: Harvard Business Review July-August 1985, S. 133-138.

Viscusi, W. Kip (1991): Product and Occupational Liablity, in: Journal of Economic Perspectives 5/1991, H. 3, S. 71-91.

Viscusi, W. Kip (1992): Fatal Tradeoffs - Public and Private Responsibilites for Risk, New York u. a. 1992.

Vogelgesang, K. (1987): Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Vogelsang, I. (1995): Interconnection of Telecommunications Networks in the UK, Diskussionsbeitrag Nr. 140 des WIK, Bad Honnef 1995.

Volle, P. (1995): Aufwand und Ertrag bei Datensicherungsmaßnahmen gemäß §9 BDSG, in: Computer und Recht 11/1995, H. 2, S. 120-124.

Voßbein, R. (1994): IT-Sicherheitsberatung: Leistungen und Preise, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 1994, H. 4, S. 18-24.

Wacker-Theodorakopoulos, C. und Kreienbaum, Ch. (1991): Das neue Umwelthaftungsrecht, in: Wirtschaftsdienst 71/1991 H. 8, S. 423-428.

Weinkopf, M. (1993): Ökonomie des ONP-Konzeptes, Diskussionsbeitrag Nr. 118 des WIK, Bad Honnef 1993.

Weishaupt, G. (1994): Mehr Schutz für Telekom-Kunden, in: Das Handelsblatt, 15. 12. 1994, S. 17.

Weitzman, M. L. (1974): Prices vs. Quantities, in: Review of Economic Studies 41/1974, S. 477-491.

Welzel, P. (1993): Datenfernübertragung: Einführende Grundlagen zur Kommunikation offener Systeme, 3. Aufl. Braunschweig 1993.

Wenders, J. T. (1987): The Economics of Telecommunications: Theory and Policy, Cambridge MA 1987.

Wicke, L. (1993): Umweltökonomie, 4. Auflage München 1993.

Wildhaber, B. (1993): Informationssicherheit: Rechtliche Grundlagen und Anforderungen an die Praxis, Zürich 1993.

Wilson, J. Q. (1980): The Politics of Regulation, in: The Politics of Regulation hrsg. von Wilson J. Q., New York 1980, S. 357-390.

Wischermann, B. (1991): Produzentenhaftung und Risikobewältigung: Eine ökonomische Analyse, München 1991.

Wolfenstetter, K.-D. (1991): TeleSec: Technische Grundlagen und organisatorische Umsetzung, in: Technikfolgenabschätzung in der Telekommunikation hrsg. von Garbe D. und Lange K., Berlin 1991, S. 123-129.

Wolfenstetter, K.-D. (1993): Datenschutz und Datensicherung in neuen Kommunikationsmedien, in: Nachrichtentechnische Zeitung 46/1993, H. 10, S. 736-744.

Zehle, K.-O. (1993): Ins Netz gegangen: Sicherheit, in: Zeitschrift für Kommunikations- und EDV-Sicherheit 1993, H. 4, S. 14-17.

Zimtl, R. (1993): Clubs, Clans und Cliquen, in: Ökonomische Verhaltenstheorie hrsg. von Ramb, B.-Th. und Tietztel, M., München 1993, S. 89-117.

FINANZWISSENSCHAFTLICHE SCHRIFTEN

Band 1 Werner Steden: Finanzpolitik und Einkommensverteilung. Ein Wachstums- und Konjunkturmodell der Bundesrepublik Deutschland. 1979.

Band 2 Rainer Hagemann: Kommunale Finanzplanung im föderativen Staat. 1976.

Band 3 Klaus Scherer: Maßstäbe zur Beurteilung von konjunkturellen Wirkungen des öffentlichen Haushalts. 1977.

Band 4 Brita Steinbach: "Formula Flexibility" - Kritische Analyse und Vergleich mit diskretionärer Konjunkturpolitik. 1977.

Band 5 Hans-Georg Petersen: Personelle Einkommensbesteuerung und Inflation. Eine theoretisch-empirische Analyse der Lohn- und veranlagten Einkommensteuer in der Bundesrepublik Deutschland. 1977.

Band 6 Friedemann Tetsch: Raumwirkungen des Finanzsystems der Bundesrepublik Deutschland. Eine Untersuchung der Auswirkungen der Finanzreform von 1969 auf die Einnahmenposition der untergeordneten Gebietskörperschaften und ihrer regionalpolitischen Zieladäquanz. 1978.

Band 7 Wilhelm Pfähler: Normative Theorie der fiskalischen Besteuerung. Ein methodologischer und theoretischer Beitrag zur Integration der normativen Besteuerungstheorie in der Wohlfahrtstheorie. 1978.

Band 8 Wolfgang Wiegard: Optimale Schattenpreise und Produktionsprogramme für öffentliche Unternehmen. Second-Best Modelle im finanzwirtschaftlichen Staatsbereich. 1978.

Band 9 Hans P. Fischer: Die Finanzierung des Umweltschutzes im Rahmen einer rationalen Umweltpolitik. 1978.

Band 10 Rainer Paulenz: Der Einsatz finanzpolitischer Instrumente in der Forschungs- und Entwicklungspolitik. 1978.

Band 11 Hans-Joachim Hauser: Verteilungswirkungen der Staatsverschuldung. Eine kreislauftheoretische Inzidenzbetrachtung. 1979.

Band 12 Gunnar Schwarting: Kommunale Investitionen. Theoretische und empirische Untersuchungen der Bestimmungsgründe kommunaler Investitionstätigkeit in Nordrhein-Westfalen 1965-1972. 1979.

Band 13 Hans-Joachim Conrad: Stadt-Umland-Wanderung und Finanzwirtschaft der Kernstädte. Amerikanische Erfahrungen, grundsätzliche Zusammenhänge und eine Fallstudie für das Ballungsgebiet Frankfurt am Main. 1980.

Band 14 Cay Folkers: Vermögensverteilung und staatliche Aktivität. Zur Theorie distributiver Prozesse im Interventionsstaat. 1981.

Band 15 Helmut Fischer: US-amerikanische Exportförderung durch die DISC-Gesetzgebung. 1981.

Band 16 Günter Ott: Einkommensumverteilungen in der gesetzlichen Krankenversicherung. Eine quantitative Analyse. 1981.

Band 17 Johann Hermann von Oehsen: Optimale Besteuerung. *(Optimal Taxation)*. 1982.

Band 18 Richard Kössler: Sozialversicherungsprinzip und Staatszuschüsse in der gesetzlichen Rentenversicherung. 1982.

Band 19 Hinrich Steffen: Zum Handlungs- und Entscheidungsspielraum der kommunalen Investitionspolitik in der Bundesrepublik Deutschland. 1983.

Band 20 Manfred Scheuer: Wirkungen einer Auslandsverschuldung des Staates bei flexiblen Wechselkursen. 1983.

Band 21 Christian Schiller: Staatsausgaben und crowding-out-Effekte. Zur Effizienz einer Finanzpolitik keynesianischer Provenienz. 1983.

Band 22 Hannelore Weck: Schattenwirtschaft: Eine Möglichkeit zur Einschränkung der öffentlichen Verwaltung? Eine ökonomische Analyse. 1983.

Band 23 Wolfgang Schmitt: Steuern als Mittel der Einkommenspolitik. Eine Ergänzung der Stabilitätspolitik? 1984.

Band 24 Wolfgang Laux: Erhöhung staatswirtschaftlicher Effizienz durch budgetäre Selbstbeschränkung? Zur Idee einer verfassungsmäßig verankerten Ausgabengrenze. 1984.

Band 25 Brita Steinbach-van der Veen: Steuerinzidenz. Methodologische Grundlagen und empirisch-statistische Probleme von Länderstudien. 1985.

Band 26 Albert Peters: Ökonomische Kriterien für eine Aufgabenverteilung in der Marktwirtschaft. Eine deskriptive und normative Betrachtung für den Allokationsbereich. 1985.

Band 27 Achim Zeidler: Möglichkeiten zur Fortsetzung der Gemeindefinanzreform. Eine theoretische und empirische Analyse. 1985.

Band 28 Peter Bartsch: Zur Theorie der längerfristigen Wirkungen 'expansiver' Fiskalpolitik. Eine dynamische Analyse unter besonderer Berücksichtigung der staatlichen Budgetbeschränkung und ausgewählter Möglichkeiten der öffentlichen Defizitfinanzierung. 1986.

Band 29 Konrad Beiwinkel: Wehrgerechtigkeit als finanzpolitisches Verteilungsproblem. Möglichkeiten einer Kompensation von Wehrungerechtigkeit durch monetäre Transfers. 1986.

Band 30 Wolfgang Kitterer: Effizienz- und Verteilungswirkungen des Steuersystems. 1986.

Band 31 Heinz Dieter Hessler: Theorie und Politik der Personalsteuern. Eine Kritik ihrer Einkommens- und Vermögensbegriffe mit Blick auf die Leistungsfähigkeitstheorie. 1994.

Band 32 Wolfgang Scherf: Die beschäftigungspolitische und fiskalische Problematik der Arbeitgeberbeiträge zur Rentenversicherung. Eine Auseinandersetzung mit der Kritik an der lohnbezogenen Beitragsbemessung. 1987.

Band 33 Andreas Mästle: Die Steuerunion. Probleme der Harmonisierung spezifischer Gütersteuern. 1987.

Band 34 Günter Ott: Internationale Verteilungswirkungen im Finanzausgleich der Europäischen Gemeinschaften. 1987.

Band 35 Heinz Haller: Zur Frage der zweckmäßigen Gestalt gemeindlicher Steuern. Ein Diskussionsbeitrag zur Gemeindesteuerreform. 1987.

Band 36 Thomas Kuhn: Schlüsselzuweisungen und fiskalische Ungleichheit. Eine theoretische Analyse der Verteilung von Schlüsselzuweisungen an Kommunen. 1988.

Band 37 Walter Hahn: Steuerpolitische Willensbildungsprozesse in der Europäischen Gemeinschaft. Das Beispiel der Umsatzssteuer-Harmonisierung. 1988.

Band 38 Ulrike Hardt: Kommunale Finanzkraft. Die Problematik einer objektiven Bestimmung kommunaler Einnahmemöglichkeiten in der gemeindlichen Haushaltsplanung und im kommunalen Finanzausgleich. 1988.

Band 39 Jochen Michaelis: Optimale Finanzpolitik im Modell überlappender Generationen. 1989.

Band 40 Bernd Raffelhüschen: Anreizwirkungen der sozialen Alterssicherung. Eine dynamische Simulationsanalyse. 1989.

Band 41 Berend Diekmann: Die Anleihe- und Darlehenstransaktionen der Europäischen Gemeinschaften. 1990.

Band 42 Helmut Kaiser: Konsumnachfrage, Arbeitsangebot und optimale Haushaltsbesteuerung. Theoretische Ergebnisse und mikroökonometrische Simulation für die Bundesrepublik Deutschland. 1990.

Band 43 Rüdiger von Kleist: Das Gramm-Rudman-Hollings-Gesetz. Ein gescheiterter Versuch der Haushaltskonsolidierung. 1991.

Band 44 Rolf Hagedorn: Steuerhinterziehung und Finanzpolitik. Ein theoretischer Beitrag unter besonderer Berücksichtigung der Hinterziehung von Zinserträgen. 1991.

Band 45 Cornelia S. Behrens: Intertemporale Verteilungswirkungen in der gesetzlichen Krankenversicherung der Bundesrepublik Deutschland. 1991.

Band 46 Peter Saile: Ein ökonomischer Ansatz der Theorie der intermediären Finanzgewalten – Die Kirchen als Parafisci. 1992.

Band 47 Peter Gottfried: Die verdeckten Effizienzwirkungen der Umsatzsteuer. Eine empirische allgemeine Gleichgewichtsanalyse. 1992.

Band 48 Andreas Burger: Umweltorientierte Beschäftigungsprogramme. Eine Effizienzanalyse am Beispiel des "Sondervermögens Arbeit und Umwelt". 1992.

Band 49 Jeanette Malchow: Die Zuordnung verteilungspolitischer Kompetenzen in der Europäischen Gemeinschaft. Eine Untersuchung aufgrund einer Fortentwicklung der ökonomischen Theorie des Föderalismus. 1992.

Band 50 Barbara Seidel: Die Einbindung der Bundesrepublik Deutschland in die Europäischen Gemeinschaften als Problem des Finanzausgleichs. 1992.

Band 51 Ralph Wiechers: Markt und Macht im Rundfunk. Zur Stellung der öffentlich-rechtlichen Rundfunkanstalten im dualen Rundfunksystem der Bundesrepublik Deutschland. 1992.

Band 52 Klaus Eckhardt: Probleme einer Umweltpolitik mit Abgaben. 1993.

Band 53 Oliver Schwarzkopf: Die Problematik unterschiedlicher Körperschaftsteuersysteme innerhalb der EG. 1993.

Band 54 Thorsten Giersch: Bergson-Wohlfahrtsfunktion und normative Ökonomie. 1993.

Band 55 Li-Fang Chou: Selbstbeteiligung bei Arzneimitteln aus ordnungspolitischer Sicht. Das Beispiel der Bundesrepublik Deutschland. 1993.

Band 56 Harald Schlee: Einkommensteuerliche Behandlung von Transferzahlungen. Zur Neuordnung der Familienbesteuerung sowie der Besteuerung von Versicherungsleistungen und Sozialtransfers. 1994.

Band 57 Alexander Spermann: Kommunales Krisenmanagement. Reaktionen baden-württembergischer Stadtkreise auf steigende Sozialhilfekosten und Einnahmenausfälle (1980-92). 1993.

Band 58 Otto Roloff / Sibylle Brander / Ingo Barens / Claudia Wesselbaum: Direktinvestitionen und internationale Steuerkonkurrenz. 1994.

Band 59 Claudia Wesselbaum-Neugebauer: Internationale Steuerbelastungsvergleiche. 1994.

Band 60 Stephanie Miera: Kommunales Finanzsystem und Bevölkerungsentwicklung. Eine Analyse des kommunalen Finanzsystems vor dem Hintergrund der sich abzeichnenden Bevölkerungsentwicklung am Beispiel Niedersachsens unter besonderer Berücksichtigung des Landkreises Wolfenbüttel und seiner Gemeinden. 1994.

Band 61 Wolfgang Scherf: Die Bedeutung des kaldorianischen Verteilungsmechanismus für die gesamtwirtschaftlichen Wirkungen der staatlichen Neuverschuldung. 1994.

Band 62 Rainer Volk: Vergleich der Vergünstigungseffekte der verschiedenen investitionsfördernden Maßnahmen. 1994.

Band 63 Hans-Georg Napp: Kommunale Finanzautonomie und ihre Bedeutung für eine effiziente lokale Finanzwirtschaft. 1994. 2., unveränderte Auflage 1994.

Band 64 Bernd Rahmann / Uwe Steinborn / Günter Vornholz: Empirische Analyse der Autonomie lokaler Finanzwirtschaften in der Europäischen Gemeinschaft. 1994.

Band 65 Carsten Kühl: Strategien zur Finanzierung der Altlastensanierung. 1994.

Band 66 Stephan Boll: Intergenerationale Umverteilungswirkungen der Fiskalpolitik in der Bundesrepublik Deutschland. Ein Ansatz mit Hilfe des Generational Accounting. 1994.

Band 67 Karl Justus Bernhard Neumärker: Finanzverfassung und Staatsgewalt in der Demokratie. Ein Beitrag zur konstitutionellen Finanztheorie. 1995.

Band 68 Christian Haslbeck: Zentrale versus dezentrale Internalisierung externer Effekte bei unvollständiger Information. 1995.

Band 69 Regina Müller: Horizontale oder vertikale Transfers zur Durchsetzung eines horizontalen Finanzausgleichs. 1995.

Band 70 Christian Hockenjos: Öffentliche Sportförderung in der Bundesrepublik Deutschland. Darstellung und finanztheoretische Analyse. 1995.

Band 71 Manfred Rosenstock: Die Kontrolle und Harmonisierung nationaler Beihilfen durch die Kommission der Europäischen Gemeinschaften. 1995.

Band 72 Christian Rüsch: Wohnungsbau- und Wohneigentumspolitik im Rahmen der Einkommensteuer. Eine Analyse unter steuersystematischen, verteilungspolitischen und fiskalischen Aspekten. 1996.

Band 73 Stephan Winters: Die kollektive Vorsorge für den Pflegefall im Alter. Eine Untersuchung am Beispiel der gesetzlichen Pflegeversicherung in den Niederlanden. 1996.

Band 74 Knut Blind: Allokationsineffizienzen auf Sicherheitsmärkten: Ursachen und Lösungsmöglichkeiten. Fallstudie: Informationssicherheit in Kommunikationssystemen. 1996.